국정원 국민해킹사찰대응 시민사회단체 일동

수 신 각 언론사 사회부, 정치부

발 신 국정원 국민해킹사찰대응 시민사회단체 일동
(담당 : 진보네트워크센터 장여경 019-339-2599, 참여연대 이은미 010-3341-9189)

제 목 [보도자료] 국정원의 해킹사찰에 대한 국민고발 기자회견

날 짜 2015. 7. 30. (총 2 쪽, 고발장 별첨)

보 도 자 료

국정원의 해킹사찰에 대한 국민고발 기자회견

일시 및 장소 : 7월 30일(목), 오전 11시 30분, 서울중앙지방검찰청 앞 (법원삼거리)

1. 취지와 목적

- 국정원의 불법적인 해킹 프로그램 구입하고 이를 내국인을 대상으로 사용한 행위를 검찰에 고발하고자 함
- 7/27일(월)~29일(수)까지 온라인상에서 국민고발인을 공개모집하여, 참여의사를 밝힌 2,786명의 시민과 41개의 시민사회단체가 함께 고발.

2. 고발 개요

○ 혐 의 : “통신비밀보호법“, “정보통신망 이용촉진 및 정보보호 등에 관한 법률“ 위반

○ 고발인 : 2,786명의 시민, 41개의 시민사회단체

○ 피고발인 : 원세훈 전 원장부터 현재 국정원장까지 국정원의 국민해킹 책임자 및 실행자

3. 기자회견

○ 제목 : 국정원의 해킹사찰에 대한 국민고발 기자회견

○ 주최 : 국정원 국민해킹사찰대응 시민사회단체 일동 (가만히 있지 않는 경산청년 모임, 가만히있으라 with 제주, 거제서명팀, 검은티행동, 경기시흥촛불, 고양세실(고양시 세월호 실천 모임), 광화문TV, 노원 416의 약속, 노후희망유니온, 대구 반야

월 세월호 유가족과 함께 하는 사람들, 대구경북 별들과의 동행, 리멤버 0416, 민주노총, 민주사회를 위한 변호사모임, 민주전역시민회, 민주주의국민행동, 민주화를위한전국교수협의회, 부정선거진상규명시민모임, 분당사랑방 세월호소모임, 사회민주당창당모임, 서대문416네트워크, 세대행동(세월호와 대한민국을 위해 행동하는 사람들), 세월호 원주대책위, 세월호를 기억하는 용인시민모임, 아시아의 친구들, 엄마의 노란손수건, 의정부 세월호 대책회의, 이화여대민주동문회, 인천서명팀(부평 검암 구월), 전국교수노조, 진보네트워크센터, 참여연대, 천주교인권위원회, 초아민주모임, 표현의자유와언론탄압공동대책위원회, 풀뿌리시민네트워크, 한국비정규교수노조, 한국진보연대, 한국청년연대, 한신대 총학생회, 함께하는 이웃 총 41 개 시민사회단체)

○ 참가자

- 사회 : 장여경 (진보네트워크센터 활동가)
- 주요참석자: 박석운(한국진보연대 공동대표), 송주명(민주화를위한전국교수협의회 상임의장), 이종회(진보네트워크센터 대표), 이호중(천주교인권위원회 상임이사), 장유식(참여연대 행정감시센터 소장), 최종진(민주노총 수석부위원장)

○ 향후 계획

- 1차 고발 후 8월 12일까지를 시한으로 2차 고발운동 진행
- 2차 고발장 접수는 8월 13일 예정
- 2차는 온, 오프라인으로 진행

○ 문의 : 장여경 (진보네트워크센터) 019-339-2599,
이은미 (참여연대) 010-3341-9189

4. 귀 언론사의 취재와 보도를 요청합니다. 끝.

고 발 장

고 발 인　　<별지1 대표고발인 명단> 및 <별지2 국민고발단 명단> 기재와 같음

위 고발인들의 대리인 <별지3> 기재와 같음

피고발인　　1. 원세훈(전 국가정보원장, 현재 서울구치소 수감 중)
2. 남재준(전 국가정보원장)
3. 이병기(전 국가정보원장, 현 대통령 비서실장)
4. 이병호(현 국가정보원장)
5. 김동현
6. 성명불상자(피고발인1 재임시절 국가정보원 2차장)
7. 성명불상자(피고발인6 이후의 국가정보원 2차장)
8. 김모(피고발인1 재임시절 사이버보안국장)
9. 성명불상자(피고발인7 이후의 사이버보안국장)
10. 이종명(전 국가정보원 3차장)
11. 성명불상자(피고발인9 이후의 국가정보원 3차장)
12. 성명불상자(피고발인1 재임시절 과학정보국장)
13. 성명불상자[최근 자살한 임모씨와 같이 일했던 연구개발단(팀) 소속 직원들)]
14. 허손구(주식회사 나나테크 대표이사)
서울 마포구 신공덕동 5-75 동성빌딩 3층

고 발 취 지

고발인들은 피고발인들에 대하여 통신비밀보호법위반 등의 혐의로 고발하오니 철저히 수사하여 엄히 처벌하여 주기 바랍니다.

고 발 이 유

Ⅰ. 고발인들 및 피고발인들의 지위

1. 고발인들은 대한민국의 국민들로서 우리나라의 민주주의를 발전시키기 위해서 국가정보원이 행했을 것으로 의심되고 있는 국민을 대상으로 한 사찰, 해킹의 진상을 규명하고 책임자를 처벌하고자 하는 자이고,

2. 피고발인1은 2009. 2.부터 2013. 3.까지 제30대 국가정보원장으로, 피고발인2는 2013. 3.부터 2014. 5.까지 제31대 국가정보원 원장으로, 피고발인3은 2014. 7.부터 2015. 2.까지 제32대 국가정보원장으로, 피고발인4는 2015. 3.부터 현재까지 제33대 국가정보원장으로 재직한 자들로서 국가정보원이 해킹 팀으로부터 RCS를 구입하여 운영한 자들이며,

3. 피고발인5는 국가정보원 직원으로 보이는 자이며 이탈리아 해킹 팀으로부터 RCS를 구입하거나 그 성능의 개선 등을 요구한 것으로 보이는 자입니다.

4. 피고발인6은 피고발인1이 국정원장으로 재직할 당시 국정원 2차장으로 재직하며 RCS를 최초로 구매한 것으로 보이는 자이며,

5. 피고발인7은 피고발인6 이후 국정원 2차장으로 재직하면서 RCS를 관리, 사용하여 왔을 것으로 보이는 자들이고,

6. 피고발인8은 피고발인6이 국정원 2차장으로 재직할 당시 피고발인6의 휘하 사이버보안국장으로 근무하던 자로 RCS 구매계약을 책임졌던 것으로 보이는 자이며,

7. 피고발인9는 피고발인8 이후의 사이버보안국장으로 피고발인8과 같은 역할을 수행했을 것으로 보이는 자이고,

8. 피고발인10은 피고발인1이 국정원장으로 재직할 당시 국정원 3차장으로 근무하던 자로 휘하에 과학정보국, 연구개발팀(단)을 운용하면서 RCS의 구매와 연구, 운용에 관여한 것으로 보이는 자이고,

9. 피고발인11은 피고발인10 이후 국정원 3차장으로 재직하면서 피고발인10과 같은 역할을 수행했을 것으로 보이는 자이며,

10. 피고발인12는 피고발인1이 국정원장을 역임한 이후 국정원에서 과학정보국장을 역임하며 RCS를 연구, 개발, 관리 및 운용한 것으로 보이는 자들이고,

11. 피고발인13은 최근 스스로 목숨을 끊은 국정원 직원 임모씨와 같이 과학정보국 산하 연구개발팀(단)에서 RCS를 구매하고, 연구하며, 사용한 것으로 보이는 자들이며,

12. 피고발인14는 주식회사 나나테크의 대표이사로서 국가정보원이 이탈리아 해킹 팀(Hacking Team)(이하 “해킹 팀”이라고만 하겠습니다)으로부터 ‘RCS(Remote Control System)’(이하 “RCS”라고만 하겠습니다)을 구입하거나 그 성능의 개선 등을 요구할 때 이를 대리한 자입니다.

Ⅱ. 최근의 논란과 관련 법령

1. 배경사실

2015. 7. 5. 누군가가 해킹 팀의 내부자료를 해킹을 통해 확보한 후 인터넷에 공개를 하였습니다. 이 내부자료에는 RCS의 소스코드를 비롯하여 RCS를 구매한 나라와 구체적인 구매내역 등이 담겨있었습니다.

RCS는 사용자의 PC나 핸드폰에 원격조종을 가능하게 하는 스파이웨어를 침투시킨 다음, 그것과 연결된 컴퓨터시스템을 통하여 사용자의 PC나 스마트폰을 원격조종하여 정보를 빼내는 방식으로 작동하는 것으로 알려졌습니다. RCS의 기능에 대해서는 대략 아래와 같이 알려져 있습니다.

①컴퓨터나 스마트폰의 사용자가 인터넷에 접속하는 경우에 정보통신망을 통해서 이루어지는 전화통화나 메시지 송수신의 내용은 실시간으로 감시자에 전달된다.

②감시자는 스마트폰에 내장된 카메라를 원격조종하여 사용자 몰래 사용자의 상태나 주변상황에 관한 화상정보를 전송받을 수 있으며, 통화내용을 몰래 녹음하여 전송하는 것도 가능하다.

③ 더 나아가서, 감시자는 컴퓨터나 스마트폰에 저장된 정보도 사용자 몰래 검색하고 수집할 수 있으며, 사용자가 사용하는 아이디나 비밀번호도 수집할 수 있다.

사용자가 데이터를 암호화 행태로 저장하는 경우에도 감시자는 사용자가 특정 시점에 데이터를 사용하는 것과 동일한 방법으로 그 데이터에 접근할 수 있기 때문에 암호화되기 전 단계에서 정보를 수집할 수 있다는 점도 RCS 의 특징입니다.

RCS는 그 작동을 가능하게 하는 스파이웨어를 사용자의 컴퓨터나 스마트폰에 침투시켜야 합니다. 국정원과 이탈리아 해킹 팀 간의 이메일 등을 통해 지금까지 드러난 바에 따르면, 사용자의 컴퓨터나 스마트폰에 스파이웨어를 감염시키는 방법으로는 다음의 기술적 방법이 사용될 수 있다고 합니다.

① 피싱URL, 스미싱URL로 접속하도록 하는 방법

② MS 원드파일이나 파워포인트파일 등으로 위장하여 해당 파일을 다운로드할 때 스파이웨어를 설치하는 방법

③ 특정 앱을 설치하도록 하여 스파이웨어가 설치되도록 하는 방법

④ 무선랜인 와이파이망을 조작해 와이파이접속 시 스파이웨어가 설치되도록 하는 방법

피싱이나 스미싱 방식은 특정한 대상자에게 문자나 메일을 보내는 방식이라서 대상자를 특정하여 작동하는 것인 반면에, 앱설치 방식이나 와이파이망 침입 형태의 방식은 불특정 다수의 시민을 상대로 스파이웨어를 감염시킬 수 있습니다.

2. RCS 관련 의혹

해킹 팀으로부터 유출된 내부자료에는 국가정보원도 해킹 팀의 고객이었고, RCS를 구입한 것으로 볼 수 있는 자료들도 포함되어 있었습니다. 이에 아래와 같은 논란과 의혹이 제기되고 있는 상황입니다.

1. 국가정보원은 주식회사 나나테크를 통해 휴대폰과 컴퓨터 등을 감청하는 것을 넘어서서 해킹할 수 있는 RCS를 아무런 통보절차 없이 도입하였다 (행위1).

2. 국가정보원은 이렇게 도입한 RCS를 내국인을 대상으로 사용하였다(RCS유포 혹

은 감염+감청 혹은 그를 넘어선 정보, 비밀 침해행위)(행위2).

이러한 의혹이 사실이라면 피고발인들은 대략적으로 아래와 같은 법령을 위반한 것으로 보입니다.

행위	위반법령	비고
행위1	통신비밀보호법(이하 "통비법") 제10조의2 제2항	국회 정보위원회에 대한 통보의무 위반
행위2	정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정통망법") 제48조 제2항	악성프로그램의 전달 또는 유포
	정통망법 제48조 제1항	정당한 접근권한 없이 정보통신망에 침입
	정통망법 제49조	타인의 비밀침해
	통비법 제7조 제1항, 제3조	대화를 감청하려는 경우 고등법원 수석부장판사의 허가 혹은 대통령의 승인을 얻을 의무 위반
	국정원법 제11조 제1항	직권을 남용하여 사람의 권리행사 방해

여기서 국정원법위반(직권남용)이 성립하기 위해서는 피고발인들이 직권을 남용하여 사람의 권리행사를 방해하여야 합니다. 우리 헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다."고 하여 국민의 사생활의 비밀을 보장하고 있고, 제18조는 "모든 국민은 통신의 비밀을 침해받지 아니한다."고 하여 통신의 비밀을 보장하고 있습니다. 이로부터 국민은 자신의 사생활의 비밀을 지키고, 통신의 비밀을 지킬 권리를 인정받고 있다고 보아야 합니다. 그리고 이러한 권리에는 RCS와 같은 해킹 프로그램에 의해 자신의 사생활의 비밀과 통신의 비밀을 침해당하지 않고 지킬 수 있는 권리가 당연히 포함된다고 할 것입니다. 독일의 경우도 해킹 프로그램을 통한 사생활의 비밀과 통신의 비밀 침해를 막기 위해 독일 연방헌법재판소는 "정보기술 시스템의 기밀성과 무결성을 보장받을 수 있는 권리(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)"라는 개념을 도입하였습니다.[1] 따라서 국정원이 RCS를 사용하여 사람이 사용하는 휴대폰 혹은 컴퓨터 등에 저장되어 있는 정보를 획득하거나 침해하면 직권남용행위에 해당할 것입니다.

Ⅲ. 국가정보원(피고발인4)의 해명

이러한 의혹에 대해 피고발인4는 현직 국가정보원장으로서 2015. 7.14. 국회 정보위원회에 출석하여 "2012. 1.과 7., 이탈리아 해킹 팀으로부터 총 20명분의 RCS를 구입했고 연구용 혹은 해외에서 필요한 대상에 사용할 목적이었다."고 해명했습니다.

1) BVerfG v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07. 이 결정은 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항에서 헌법보호청에게 정보기술시스템에의 비밀 접근을 허용하는 규정을 도입한 것(이 규정은 2006년 12월 20일 발효)에 대한 헌법소원 사건에 대한 것이다.

Ⅳ. 위법행위에 대한 여전한 의혹

그러나 피고발인4의 위와 같은 해명에도 불구하고 여전히 의혹은 남아 있습니다. 그 구체적인 내용은 아래와 같습니다.

1. RCS 구입시기와 구입량

가. 2012. 3., 9., 12.의 추가 구매의혹

위에서 본 바와 같이 피고발인4는 2012. 1.과 7.에만 RCS를 구매한 것처럼 해명하였습니다. 그러나 국가정보원(이하 “국정원”이라고만 하겠습니다)은 총선 한 달 전인 같은 해 3. 14.과 대선 10여 일 전인 12. 6.에도 30개 이상의 해킹 프로그램 계정을 구입한 사실이 유출된 해킹팀 이메일에서 드러났습니다. 또 같은 해 9.에도 4개의 '어노니마이저(추적을 따돌리는 기능의 프로그램)' 라이센스를 주문하였습니다(참고자료1 참조).

국정원의 해킹 프로그램 구매 대행 또는 중개를 한 중소 무역 업체 주식회사 나나테크(이하 “나나테크”라고만 하겠습니다)는 2012. 3. 14. 해킹 팀 측에 '새 주문(대량)'이라는 제목의 메일을 보냅니다. 이후 해킹 팀과 나나테크 사이에 메일로 오간 대화를 보면, 나나테크는 35개의 라이센스를 추가 주문했고 총 11만 유로를 가격으로 지불하는 것으로 돼 있습니다.

나나테크는 같은 해 9. 10.에도 "고객으로부터 '어노니마이저' 소프트웨어 라이센스 추가 주문이 있다"며 "그(고객)는 4개의 소프트웨어 라이센스를 필요로 한다"는 메일을 보냈습니다. 나나테크는 "귀사가 소프트웨어 라이센스 2개에 1만5000유로라는 가격을 제시했는데, 고객은 할인을 원한다"며 가격 흥정을 시도하기도 했습니다. 참고로 '어노니마이저'란 해킹 팀의 해킹 프로그램 'RCS(리모트 컨트롤 시스템)'의 일부로 보입니다. 해킹 팀이 다른 손님들과 주고받은 이메일 등을 참조하면 RCS는 RCS-어노니마이저(RCS-ANM)와 RCS-원격감염(RCS-RMI. Remote Mobile Infection) 등으로 나뉘어 거래되기도 했습니다(참고자료1 참조).

또 나나테크는 2012. 12. 19. 있었던 대통령선거를 13일 앞둔 같은 달 6.에도 '새 주문(긴급)'이라는 메일을 해킹팀에 보냅니다. 이에 대한 해킹 팀의 답신과 나나테크의 재답신 등을 보면, 나나테크는 30개의 라이센스를 추가 주문하면서 '한 달만 임시로 사용하는 것도 가능한가'라고 묻기도 했고, "고객이 30개의 타깃을 올해 예산으로 구입하고 싶어한다"며 유지 보수 비용을 15%로 해달라고 요구하기도 했습니다(참고자료1 참조).

이 같은 2012. 3., 9., 12.의 RCS구입은 피고발인4의 국회 정보위원회에서의

발언에 정면 배치되는 것입니다. 따라서 국정원이 RCS를 언제, 얼마나 구입했는지에 대해서는 명확히 해명되었다고 볼 수 없습니다.

나. 2014년 추가 구매의혹

그리고 피고발인4의 해명과 달리 2014.에도 국정원이 RCS를 구입하였다는 의혹이 제기되고 있습니다. 유출된 해킹 팀 자료 가운데 2010년부터 최근까지 고객별 매출현황을 담고 있는 '고객 개요 리스트 20150603'(Client Overview_list_20150603) 파일을 분석해보며, 국정원(SKA라는 이름 사용)과 해킹 팀이 거래한 액수는 모두 68만6400유로(약 8억6000만원)에 이릅니다. 이는 해킹 프로그램 구매액과 기존에 구매한 프로그램의 유지보수 비용을 합한 금액으로, 유지보수 비용을 뺀 구매 금액은 52만6000유로입니다. 이 가운데 44만8000유로는 국정원이 말한 RCS를 구매했던 2012.에 지불한 액수입니다. 거래 영수증을 보면, 국정원은 RCS를 최초 도입했던 2012. 1.에 39만유로, 추가 구매가 이뤄진 7.에 5만8000유로를 지불한 것으로 나옵니다. 그런데 둘을 합해도 총 구매액에서 7만8000유로가 부족한데, 이와 관련된 거래는 2014년에 추가로 이뤄졌던 것으로 보입니다. 2014. 11. 5.자 구매 영수증을 보면, 국정원은 '원격공격시스템'(Remote Attack System) 구매 비용으로 7만8000유로를 지급한 것으로 나옵니다. 이는 그 동안 해킹 프로그램으로 언급되던 RCS와 다른 명칭의 프로그램입니다. 그런데 구매 시점 전후로 국정원과 해킹 팀 사이에 오간 전자우편을 보면, '원격공격시스템'(Remote Attack System) 역시 상대방 스마트폰 등을 해킹하기 위해 쓰이는 스파이웨어로 추정됩니다. 그 이유는 구매 시점인 2014. 11. 무렵 국정원 직원인 데빌에인절(전자우편 아이디 데빌에인절1004·devilangel1004@gmail.com)이 이 프로그램을 이용해 안드로이드 폰을 해킹할 수 있는지, 대상 목표물의 정보가 해킹팀 쪽에 노출되지는 않는지 등을 꼼꼼하게 따졌기 때문입니다(참고자료2 참조). 이러한 국정원의 해킹프로그램 구입 현황을 종합해보면 아래 그림과 같을 것입니다.

국가정보원의 연도별 해킹팀 해킹 프로그램 구매 현황

출처: 해킹팀 유출 자료

	2012	2013	2014	2015	합계
구매비	44만8000유로 (5억6000만원)	-	7만8000유로 (1억원)		52만6000유로 (6억6000만원)
유지보수비	-	5만8850유로 (7400만원)	6만7700유로 (8500만원)	3만3850유로 (4200만원)	16만400유로 (2억100만원)

국가정보원의 연도별 해킹팀 해킹 프로그램 구매 현황

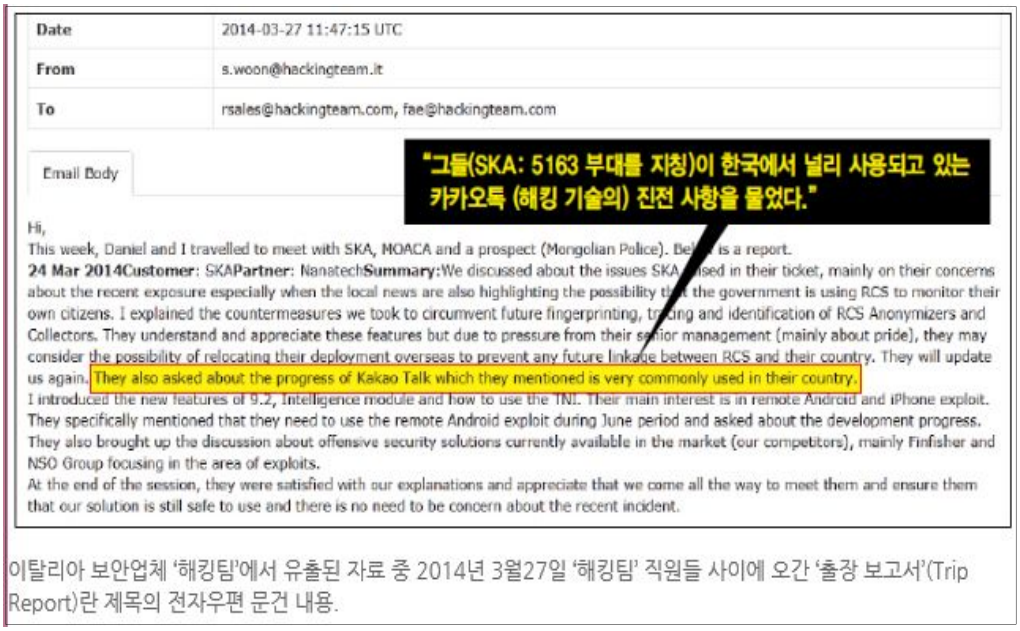
따라서 이 부분에 관한 의혹 역시 아직 해명되지 않았다고 할 것입니다.

2. 내국인을 대상으로 한 사용여부 및 그 대상의 범위

가. 내국인 대상으로 한 사용여부

피고발인4는 이미 밝힌 바와 같이 RCS를 구입하였지만 연구용 등으로만 사용하였을 뿐 내국인을 대상으로 사용한 바가 없다고 밝힌 바 있습니다. 그러나 아래와 같은 정황은 국정원이 RCS를 내국인을 대상으로 사용하였을 것이라고 합리적으로 의심하게 합니다.

첫째, 2014. 3. 27. 해킹 팀 직원들 사이에 오간 '출장 보고서'(Trip Report)란 제목의 전자우편(이메일)에서 국정원은 카카오톡을 해킹하길 원했다는 내용이 나왔습니다. 이어 '출장 보고서'(Trip Report)는 "한국이 이미 요청했던, 자국에서 가장 일반적으로 사용되는 카카오톡에 대한 (해킹 기능 개발) 진행 상황에 대해 물었다"고 적혀 있습니다. 이 이메일 보고 내용에 답변한 또 다른 해킹 팀 직원은 "이미 우리 (해킹팀의) 연구개발팀에 카카오톡에 대한 내용을 지시했다"며 "카카오톡 건에 대한 빠른 일처리를 재촉하고 있다"고 밝혔습니다(참고자료3 참조). 국내 대표적인 메신져에 대한 지속적이고 강한 관심은 RCS가 국내에서 사용되었을 것이라고 추측하게 합니다.



Date	2014-03-27 11:47:15 UTC
From	s.woon@hackingteam.it
To	rsales@hackingteam.com, fae@hackingteam.com

Email Body

Hi,
This week, Daniel and I travelled to meet with SKA, MOACA and a prospect (Mongolian Police). Be[illegible] is a report.
24 Mar 2014Customer: SKA**Partner**: Nanatech**Summary**:We discussed about the issues SKA [illegible]sed in their ticket, mainly on their concerns about the recent exposure especially when the local news are also highlighting the possibility t[illegible] the government is using RCS to monitor their own citizens. I explained the countermeasures we took to circumvent future fingerprinting, t[illegible]ding and identification of RCS Anonymizers and Collectors. They understand and appreciate these features but due to pressure from their se[illegible]ior management (mainly about pride), they may consider the possibility of relocating their deployment overseas to prevent any future linkabe between RCS and their country. They will update us again. They also asked about the progress of Kakao Talk which they mentioned is very commonly used in their country.
I introduced the new features of 9.2, Intelligence module and how to use the TNI. Their main interest is in remote Android and iPhone exploit. They specifically mentioned that they need to use the remote Android exploit during June period and asked about the development progress. They also brought up the discussion about offensive security solutions currently available in the market (our competitors), mainly Finfisher and NSO Group focusing in the area of exploits.
At the end of the session, they were satisfied with our explanations and appreciate that we come all the way to meet them and ensure them that our solution is still safe to use and there is no need to be concern about the recent incident.

이탈리아 보안업체 '해킹팀'에서 유출된 자료 중 2014년 3월27일 '해킹팀' 직원들 사이에 오간 '출장 보고서'(Trip Report)란 제목의 전자우편 문건 내용.

둘째, 국정원은 스마트폰 국내용 모델 해킹에 초점을 맞췄습니다. 2013년 2월 갤럭시S3 국내 모델을 이탈리아에 보내 몰래 음성녹음이 가능한지 살펴달라고 주문합니다. '맞춤 해킹'을 의뢰한 겁니다. 외국에서 출시된 모델은 기본 애플리케이션이 국내용과 다릅니다. 국정원이 타깃으로 삼은 감시 대상자가 국내용 모델을 쓰고 있다는 얘깁니다(참고자료4 참조). 이후로도 국정원은 갤럭시 최신형이 나올 때마다 기술 지원을 요청했습니다. 가장 최근인 지난 1일 '해킹팀'이 직원들끼리 주고받은 전자우편 내용을 보면 에스케이에이(SKA·국정원 지칭)가 집요하게 국내 최신 스마트폰에 대한 공격 기능을 요구한 정황이 확인됩니다. 메일에는 "에스케이에이의 요구가 까다롭다"며 "삼성 갤럭시 탭2, 삼성 GT-I9500, 삼성 SHV-E250S 등에 대한 해킹이 필요하다"는 대목이 눈에 띕니다(참고자료5 참조). 국내에서 많이 사용되는 핸드폰 기종 그것도 국내용 모델의 해킹에 관심이 많았다는 것 역시 RCS가 국내에서 사용되었을 것이라는 의심을 가지게 합니다.

셋째, 안랩의 'V3 모바일 2.0'과 같은 국내용 백신을 회피하기 위한 방법을

묻기도 했습니다(참고자료4 참조). 국내용 백신을 피하여야 한다고 요청한 것은 RCS가 국내에서 사용되었을 것이라는 추론을 가능하게 해줍니다.

넷째, '서울대 공대 동창회 명부'라는 제목의 워드 파일, <미디어오늘> 기자를 사칭한 천안함 보도 관련 문의 워드 파일에 악성코드를 심어달라고 요청했습니다. 천안함 관련 연구진, 서울대 출신 고위관계자 등이 감시 대상자였을 가능성이 제기됩니다(참고자료4 참조).

다섯째, 국정원이 해킹팀 쪽에 '악성 코드를 심어 달라'며 보낸 설치 파일 링크를 살펴보면 △네이버 맛집 소개 블로그 △벚꽃축제를 다룬 블로그 △삼성 업데이트 사이트를 미끼로 내건 주소가 나옵니다. 일반인들이 흔히 누를 법한 링크들입니다. 메르스가 극성을 부리던 지난 6월에는 '메르스 정보 링크'를 위장한 악성코드를 요청하기도 했습니다(참고자료4 참조). 이러한 설치 파일 링크는 외국인들이 클릭할 것으로 보기 어려운 것들입니다. 따라서 이 역시 RCS가 국내에서 사용되었을 것이라는 점을 보여줍니다.

나. 그 대상의 범위

피고발인4는 20명분의 RCS만 구입하였기에 설사 실전용으로 RCS가 사용되었다고 하더라도 그 정도 수의 사람만을 대상으로 하였을 것처럼 주장하였습니다. 그러나 이러한 해명 역시 제기되고 있는 다수자에 대한 사용의혹을 해명하지 못하고 있습니다. 그러나 전문가들은 20개의 RCS를 사용하면서 대상을 변경하면 되기에 20명분의 RCS를 구입했다는 이야기는 결국 동시 감시 대상이 20명이라는 의미밖에 없다고 주장하고 있습니다.

실제로 국정원이 RCS를 사용하며 어느 정도 인원을 감시했는지 살필 수 있는 단서가 있는데 그 중 하나가 바로 피싱 URL입니다. RCS를 사용하기 위하여는 RCS를 대상자의 핸드폰 등에 설치하여야 하는데 이를 위하여 사용되는 것이 바로 피싱 URL입니다. 그런데 피싱 URL의 경우 하나의 피싱 URL은 특정인 한 명에게만 전송할 수 있기 때문에 URL 생성 횟수는 안드로이드 스마트폰 해킹을 시도한 횟수이기도 합니다. 그런데 국정원은 지난해 12월 5일부터 올해 6월 29일까지 약 7개월 동안 50여 차례 제작을 요청했고, 이렇게 생성된 피싱 URL은 총 239개였습니다. 이 중 44개의 경우 '테스트용'임을 명시하였기에 대략 195개의 실전용 피싱 URL이 생성되었고, 이는 195명을 대상으로 한 해킹시도가 있었다는 것을 의미합니다(참고자료6 참조).

또 하나의 단서는 바로 해킹 팀이 보유하고 있는 서버의 로그기록입니다. 국정원이 보낸 피싱 URL을 누르면 이 서버에 접속, 스파이웨어에 감염되는 동시에 스파이웨어를 전송한 서버에는 접속한 기기의 IP가 남게 되기 때문입니다. 언론보도에 따르면 국회 정보위원회 야당 간사인 신경민 의원은 이탈리아 해킹팀 유출자료를 분석한 결과, 로그파일에 한국 인터넷 IP주소 138개가 존재하는 것을 확인했다고 합니다. 또한 신 의원은 "한국 IP주소 138개가 발견됐고, 중복 건수를 포함하면 2300건 정도"라면서 "(할당 기관은)

KT나 서울대, 한국방송공사같은 공공기관이고 다음카카오같은 일반 기업도 있다"고 말했다고 합니다(참고자료7 참조). 이러한 주장이 맞다면 피고발인4가 주장하는 대로 '연구개발'과 '대북용'이라거나 고작 20명을 대상으로 했다는 것은 거짓말일 가능성이 상당히 높아 보입니다.

3. 소결

이와 같이 피고발인4의 해명에도 불구하고 피고발인들의 위법행위들에 대한 의혹은 제대로 해명되지 않고 있으며 오히려 피고발인들이 위법행위를 했을 것이라고 생각하게 하는 수많은 정황과 증거들이 존재하고 있는 상황입니다.

Ⅵ. 피고발인5와 관련된 의혹

국정원이 해킹 팀과 RCS 구매계약을 체결할 때 사용했던 이메일 아이디 '데블엔젤'(devilangel1004)'입니다. 그런데 최근 이와 유사한 명칭을 사용하는 블로그(devilangel1004.blogspot.kr)가 발견됐습니다. 그런데 이 블로그 계정을 통해 무료 앱을 이용하면 스파이웨어가 설치되도록 돼있어 이 블로그가 국정원과 관련 있는 것은 아니냐는 의혹이 일고 있습니다. 이 블로그의 운영자가 바로 피고발인5['김동현'(DONG-HYEON KIM)이라는 사람]입니다. 언론보도에 의하면 피고발인5는 이 블로그 계정을 통해 구글 플러스를 이용하여 안드로이드 스마트폰용 TV, 영화, 애니메이션, 일본드라마 앱을 소개하는 사이트를 공유했다고 합니다. 해당 앱 사이트에 올라온 것은 정상적인 구글 플레이 스토어 마켓을 통하지 않고 유통되는 안드로이드 스마트폰용 앱 설치 파일(APK)들이었는데, 겉보기에는 일반 앱으로 보이지만 스파이웨어가 숨어 있었다고 합니다. 새정치민주연합의 김광진 의원실이 컴퓨터 공학 전문가와 함께 이 앱 사이트에 올라온 앱 중 '영화천국'을 다운받아 분석한 결과, 이 앱에는 ▲ GPS 현재위치 좌표 추적 ▲ 오디오 녹음 ▲ 카메라 촬영 ▲ 데이터를 특정한 주소로 송신할 수 있는 스파이웨어가 있었다는 것입니다(참고자료8 참조). 이러한 사실에 기반하여 보면 피고발인5는 국정원 직원 혹은 민간인 조력자로서 국정원이 해킹 팀으로부터 RCS를 구매할 수 있도록, 그리고 그 후 이를 이용할 수 있도록 한 자로 보입니다.

Ⅶ. 피고발인들의 위법행위 및 피고발인들에 대한 수사 및 처벌의 필요성

1. 피고발인들의 위법행위

위에서 살핀 바와 같이 피고발인4의 해명에도 불구하고 국정원은 해킹 팀으로부터 구매한 RCS를 '연구용' 혹은 '해외에 있는 사람을 대상으로'만 사용한 것은 아니라고 보입니다. 국내 민간인들을 대상으로 사용한 것으로 보입니다. 이 과정에서 피고

발인1 내지 4는 각 시기 별 국정원장으로 RCS의 추가 구매, 연구, 이용에 대한 최종 책임자와 지시자로서의 역할을 했을 것입니다. 피고발인1은 국정원이 최초로 RCS를 구매하였을 당시 국정원장으로 그 구매에 대한 결정과 지시를 하였을 것으로 보이기에 RCS의 도입과 사용과정의 불법에 대해서 잘 알고 있었을 것입니다. 피고발인2는 임명 초기에 위와 같은 행위들을 알지 못했다고 하더라도 1)2014. 3. 이미 RCS의 사용에 대한 의혹제기가 국내에서도 있었고, 2)이 의혹제기 직후 국정원이 해킹 팀에 "보안이 생명인데 폭로 탓에 문제가 생겼다. 해킹 프로그램을 가상사설서버(VPS)로 옮기자"고 제안하기도 하였던 것(참고자료9) 등에 비추어 보면 RCS의 불법사용에 대해 알게 되었다고 보아야 할 것입니다. 당연히 피고발인3 및 5는 위와 같은 의혹제기 이후 임명되었기에 임명될 때부터 RCS의 불법사용 등에 대해 잘 알고 있었다고 보아야 합니다. 따라서 피고발인1 내지 4는 모두 RCS 도입과 사용의 불법성에 대해 알았다고 보아야 할 것입니다. 피고발인5는 위에서 살핀 바와 같이 국정원 직원 혹은 민간인 조력자로서 국정원이 해킹 팀으로부터 RCS를 구매할 수 있도록, 그리고 그 후 이를 이용할 수 있도록 한 자로 보입니다. 그리고 피고발인14는 다른 피고발인들을 도와 RCS의 구매를 대행하거나 중개하였는데, 국정원이 RCS를 구입하여 내국인 사찰에 사용할 것이라는 것을 짐작하고 있음에도 불구하고 이런 역할을 수행했던 것으로 보입니다. 따라서 피고발14는 나머지 피고발인들의 위법행위에 대한 공범이 될 것입니다.[2)]

RCS의 도입과 사용에 대해 여러 의혹이 나오지만 이 프로그램을 활용하는 국정원 내부 조직의 규모와 실체, 지휘 계통 등이 장막에 가려져 있는 상태입니다. 야당 쪽에선 피고발인1이 사이버 대응을 위해 신설했던 피고발인6 산하 사이버보안국이 그 주체가 아니냐고 보기도 합니다. 피고발인1의 재임 시절 사이버보안국장을 지낸 피고발인8은 피고발인1이 퇴임한 뒤 국정원을 나와 현재 국책연구기관의 소장을 맡고 있다고 합니다. 이 기관은 2009년 이후 국정원 출신 5명을 채용했으며, 해킹 등 사이버 보안 연구와 관련해 국정원과 긴밀한 관계를 맺고 있다고 알려져 있습니다(참고자료10). 이 주장이 맞다면 RCS의 도입과 사용에는 피고발인6과 그 이후 국정원 2차장으로 재직하였던 피고발인7, 그리고 피고발인6 밑에서 사이버보안국장을 지낸 피고발인8, 그 이후 사이버보안국장을 지낸 피고발인9 등이 RCS 관련 불법행위에 직접적으로 관여했을 것으로 보입니다. 반면에 국정원 3차장 산하 기술개발팀이 해킹 프로그램을 관리하고 있다는 이야기도 있습니다. 북한의 해킹 공격에 대응하기 위한 연구용으로 3차장 산하 기술개발팀에서 이 프로그램을 들여왔다가 국정원 내부에서 북한 공작원 등을 대상으로 실제 이 프로그램을 활용하게 됐다는 것입니다. 국회 정보위원회 소속 문병호 새정치민주연합 의원은 한 언론사에 "국정원은 (지난 7월15일) 정보위 전체회의에서 (해킹 프로그램 관리를) 현재 3차장 산하에서 하고 있다고만 말하더라"라고 하기도 하였습니다(참고자료10). 이 주장이 맞다면 피고발인1이 국정원으로 재임하던 시절 국정원 3차장이었던 피고발인10, 그 이후 국정원 3차장을 지낸 피고발인11, 피고발인10 및 피고발인11 산하 과학정

2) 나나테크는 2012년부터 해킹업체와 국가정보원의 스파이웨어 거래를 중개해왔습니다. 이 스파이웨어는 감청설비에 포함될 가능성이 높습니다. 통비법에 따르면 감청설비는 "대화 또는 전기통신의 감청에 사용될 수 있는 전자장치·기계장치 기타 설비"로 정의되어 있고, **스파이웨어를 유포하기 위해 사용하는 컴퓨터나 스마트폰이 있다면 그 자체가 전기통신의 감청에 사용될 수 있는 장치입니다**. 스파이웨어가 저장된 USB 역시 감청을 위한 장치가 될 것입니다. 미래창조과학부 인가대장을 분석한 결과 **나나테크는 2012년 이후 최근까지 어떠한 감청설비 인가도 받지 않았습니다.** 이는 **통비법 제17조 제1항 제4호, 제10조에 위배**될 여지가 큽니다. 비록 나나테크는 진정한 구매자인 국정원의 요청을 받아 RCS를 구매한 대행자이기에 위와 같은 통비법 규정을 독자적으로 위반한 것이 아니라 국정원의 위법행위를 방조한 것으로 볼 수도 있으나 위와 같은 점들에 대해서도 면밀히 살펴 보아 주시기 바랍니다.

보국장을 지낸 피고발인12 그리고 과학정보국 산하 연구개발팀에 속해 있는 그리고 최근 자살한 국정원 직원 임모씨의 동료인 피고발인13 등이 RCS 관련 불법행위에 직접적으로 관여했을 것으로 보입니다.

국정원 3차장 산하 기술개발팀이 해킹 프로그램을 관리하고 있다는 이야기도 정치권에서 흘러나오고 있습니다. 북한의 해킹 공격에 대응하기 위한 연구용으로 3차장 산하 기술개발팀에서 이 프로그램을 들여왔다가 국정원 내부에서 북한 공작원 등을 대상으로 실제 이 프로그램을 활용하게 됐다는 것이다. 국회 정보위원회 소속 문병호 새정치민주연합 의원은 “국정원은 (지난 7월15일) 정보위 전체회의에서 (해킹 프로그램 관리를) 현재 3차장 산하에서 하고 있다고만 말하더라”라고 전했습니다.

피고발인들의 행위가 만약 위와 같다면 피고발인들은 RCS의 구매와 사용과 관련하여 Ⅱ.에서 언급한 아래와 같은 법령위반이 있었다고 할 것입니다.

행위	위반법령	비고
행위1	통신비밀보호법(이하 “통비법”) 제10조의2 제2항	국회 정보위원회에 대한 통보의무 위반
행위2	정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정통망법”) 제48조 제2항	악성프로그램의 전달 또는 유포
	정통망법 제48조 제1항	정당한 접근권한 없이 정보통신망에 침입
	정통망법 제49조	타인의 비밀침해
	통비법 제7조 제1항, 제3조	대화를 감청하려는 경우 고등법원 수석부장판사의 허가 혹은 대통령의 승인을 얻을 의무 위반
	국정원법 제11조 제1항	직권을 남용하여 사람의 권리행사 방해
1. 국가정보원은 주식회사 나나테크를 통해 휴대폰과 컴퓨터 등을 감청하는 것을 넘어서서 해킹할 수 있는 RCS를 아무런 통보절차 없이 도입하였다(행위1). **2. 국가정보원은 이렇게 도입한 RCS를 내국인을 대상으로 사용하였다(RCS유포 혹은 감염+감청 혹은 그를 넘어선 정보, 비밀 침해행위)(행위2).**		

2. 피고발인들에 대한 수사 및 처벌의 필요성

위와 같은 피고발인들의 RCS 관련 불법행위에 대하여 철저히 수사하여 관련 법령을 위반한 사정이 드러날 경우 엄벌에 처해주시기 바랍니다. 국정원이 비밀정보기관이라고는 하나 국민을 위하여 봉사하여야 함은 부정할 수 없습니다. 그럼에도 불구하고 국민들 몰래 특정 정치세력을 위하여 국민을 감시하고, 국민들의 개인정보를 마음대로 훔쳐보았다는 것이 최근 의혹들의 핵심인 이상 이는 민주주의를 훼손하고 국기를 문란케 한 중범죄에 해당할 수 있습니다. 이에 대한 수사와 책임자에 대한 처벌은 당연히 민주주의를 회복하고, 국기를 바로 세우는 중차대한 일이라 할 것입니다. 한 치의 망설임도 없이 그 어느 때보다도 추상(秋霜)같은 기운으로 수사에 임해주시기를 다시 한 번 간곡히 부탁드립니다.

Ⅷ. 진상규명을 위한 진정

위에서 언급한 내용에 비하여 훨씬 더 불분명한 부분일 수는 있으나 국정원의 RCS 불법사용과 관련하여 반드시 밝혀져야 할 부분들이 있습니다. 그 중 아래와 같은 부분들에 대해서도 반드시 조사하여 진실을 규명해주길 바랍니다.

1. RCS를 이용한 국내 정치개입 혹은 선거개입 여부

피고발인1은 2011. 10. 24. 서울시장 재·보궐 선거를 앞두고 '지금 인터넷을 보시면 아시겠지만 인터넷 자체가 종북 좌파 세력들이 다 잡았는데, 점령하다시피 보이는데 여기에 대한 대책을 우리가 제대로 안 세우고 있었다. 전 직원이 어쨌든 간에 인터넷 자체를 청소한다. 그런 자세로 해서 그런 세력을 끌어내야 한다.'는 취지의 지시, 강조말씀을 하달하였습니다. 이 지시·강조 말씀 이후 4개월 뒤, 위에서 본 바와 같이 국정원은 나나테크를 중개 대행으로 내세워 RCS 구매계약을 체결했습니다. 또 이 무렵 (비록 선거개입여부에 대해서는 다툼이 있지만)정치개입을 하였다고 인정되고 있는 국정원 심리전단도 3팀 체제에서 4팀 체제, 70여 명으로 대폭 확대되었습니다(참고자료11 참조). 전체적으로 피고발인1의 의도대로 국정원이 선거개입과 정치개입으로 나서려는 모습이 강화되는 시기에 RCS 구매계약이 체결되었기에 국정원이 RCS를 정치개입과 선거개입을 위한 도구로 사용한 것은 아닌가 의심이 들 수밖에 없습니다. 뿐만 아니라 국정원이 6·4 지방선거가 포함된 기간인 '6월'을 언급하며 '안드로이드폰 해킹 공격'을 요청한 사실도 드러났습니다. 위에서 언급한 '출장 보고서'(Trip Report)는 "한국 쪽 고객(SKA)의 가장 큰 관심은 안드로이드와 아이폰에 대한 원격 공격"이라며 "특히 한국 고객은 6월에 안드로이드폰 공격에 아르시에스를 사용하는 게 필요하다며 진전 상황을 물었다"고 밝혔습니다(참고자료3 참조). 선거시기에 안드로이드폰에 대한 해킹공격을 요청했다는 것은 RCS가 선거개입에 이용되었을 것이라는 의심을 강하게 합니다. 그리고 2012. 4. 있었던 총선 직전인 3. 14. 나나테크가 35개의 해킹 회선 라이선스(감시할 수 있는 권한)를 해킹 팀에 주문하였고, 2012. 12. 있었던 대선 직전인 12. 6. 나나테크는 "일단 한달만 사용할 수 있느냐"고 물으며 라이선스 30개 추가 주문을 하기도 하였습니다(참고자료12). 이에 대해 국정원은 신청만 했을 뿐 실제로 구입하지는 않았다고 해명하기는 하였으나 이 역시 일방적 주장일 뿐이므로 관련 의혹이 모두 해명되었다고 볼 수 없습니다(참고자료13).

만약 위와 같이 국정원이 RCS를 정치개입 및 선거개입을 위하여 사용하였다면 이는 국가정보원법 제9조 제1항 및 공직선거법 제85조 제1항을 위반한 것이 될 것입니다. 따라서 이 부분에 대해서도 한 점 의혹이 남지 않도록 조사하여 주시기 바랍니다.

2. 국정원 직원 임모씨의 사망에 관한 의혹들

7. 18. 낮 12시께 국정원 직원 임모(45)씨가 용인시 처인구 이동면 화산리 한 야산

중턱에서 자신의 마티즈 승용차 안 운전석에서 번개탄을 피워 숨진 채 발견되었습니다. 그는 7. 19. 공개된 유서에서 “지나친 업무에 대한 욕심이 오늘의 사태를 일으킨 듯합니다. 정말 내국인에 대한, 선거에 대한 사찰은 전혀 없었습니다. 외부에 대한 파장보다 국정원의 위상이 중요하다고 판단하여 혹시나 대테러, 대북 공작활동에 오해를 일으킨 지원했던 자료를 삭제하였습니다. 저의 부족한 판단이 저지른 실수였습니다. 그러나 이를 포함해서 모든 저의 행위는 우려하실 부분이 전혀 없습니다.”라고 하였습니다. 그러나 그의 죽음을 두고 1)정확한 자살동기가 무엇이며, 2)죽기 전에 삭제한 자료가 무엇인지, 3)IT전문가로서 20년간 관련 분야에서 종사한 사람이 쉽게 복구할 수 있는 방법으로 자료를 삭제한 이유가 무엇인지, 4)딜리트 키를 이용하여 삭제하였다고 하는데 그렇게 삭제된 파일을 복구하는데 1주일 이상의 시간이 걸린 이유가 무엇인지 등에 대한 의혹이 끊임없이 제기되고 있는 상황입니다. 특히 본인의 업무를 ‘대테러, 대북 공작활동’이라고 하면서도 그 활동과 관련된 자료를 삭제했다는 점, 삭제를 한 후에도 죽음을 선택했다는 점에서 오히려 국정원의 RCS 구매, 사용 등과 관련된 불법성을 입증할만한 자료들이 삭제된 것은 아닌가하는 의혹이 제기되고 있는 것입니다.

특히 임모씨가 관련 자료를 삭제한 것과 관련하여서는 보다 면밀한 조사가 필요할 것으로 보입니다. 자기 증거인멸행위는 범죄가 되지 않는다는 것이 대법원의 확립된 견해이나, 임모씨가 국정원 직원이고 이는 공무원이라는 점에서 공전자기록변작죄에 해당할 가능성은 있습니다. 즉, 변작이란 기존의 기록을 부분적으로 고치거나 말소하여 기록의 내용을 변경하는 것을 말하는데(이재상 저, 형법각론 제8판 P.610~611, 2012년 박영사 간), 임모씨가 사망하였다는 점에서 임모씨에 대한 검찰 공소권은 없으나, 이를 공모하거나 교사한 사람에게는 공전자기록변작죄의 공동정범이나 교사범은 성립할 수 있을 것입니다.

형법 제227조의2(공전자기록위작·변작) 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 전자기록등 특수매체기록을 위작 또는 변작한 자는 10년 이하의 징역에 처한다. [본조신설 1995.12.29.]

고인의 죽음을 제대로 슬퍼할 수 있도록 하기 위해서라도 위와 같은 의혹들 역시 명명백백하게 밝혀져야 할 것이며, 이것은 또한 국정원의 RCS 구매 및 사용 등과 관련한 의혹들을 밝히는 데도 도움이 될 것입니다.

Ⅸ. 첨언

1. 고발인들은 이후에 추가로 드러나는 사실관계나 피고발대상자가 있을 때 그 내용을 포함하여 추가고발을 진행할 예정입니다. 뿐만 아니라 고발인들 외의 사람들도 지속적으로 관련 고발에 동참시킬 예정입니다. 그 이유는 위에서 언급했던 것과 같이 국정원이 RCS를 구매, 사용, 관리하며 벌였을 것이고 생각되는 불법행위들을 반드시 밝혀내고 그 책임자를 처벌하여 민주주의를 지키자는 것입니다.

2. 끝으로 이 고발장이 RCS의 구매와 사용과 관련하여 각 피고발인들이 언제, 어떠한 행위를 했는지 보다 구체적으로 설시할 수 있으면 수사에 그만큼 더 도움이 될 수 있겠지만 고발인들로서는 언론과 야당에서 밝히는 것 이상의 자료를 직접 얻

기 어려운 사정이 존재합니다. 고발장에 다소 부족하고 불명확한 부분이 있더라도 이러한 사정에 기인한 것임을 양지하여 주시기 바랍니다.

참 고 자 료

1. 참고자료1 프레시안, <국정원 거짓말, 2012년 '해킹 계정' 수십개 추가 구입>
2. 참고자료2 한겨레, <국정원장 '2012년에만 해킹프로그램 구매' 국회 해명 거짓>
3. 참고자료3 한겨레, <해킹 프로그램 산 국정원, '카톡 검열' 기능도 요청했다>
4. 참고자료4 한겨레, <국정원 해킹사건 총정리>
5. 참고자료5 한겨레, <국정원, 갤럭시 출시 때마다 해킹업체에 "뚫어달라">
6. 참고자료6 오마이뉴스, <국정원 스마트폰 해킹시도 '최소' 195건>
7. 참고자료7 노컷뉴스, <"해킹팀 로그기록서 다음카카오 등 韓 IP무더기 발견">
8. 참고자료8 오마이뉴스, <국정원, 무료앱 미끼로 일반인 전방위 사찰의혹>
9. 참고자료9 동아일보, <외신이 거래 폭로하자 "서버 옮겨라"… "해킹 증거 나와선 안된다" 메일>
10. 참고자료10 한겨레21, <원세훈은 계속 웃을 수 있을까>
11. 참고자료11 시사IN, <대선이 있던 그해 '시스템'이 수입됐다>
12. 참고자료12 한겨레, <국정원, 2012년 총선·대선 직전 '해킹 계정' 긴급 주문>
13. 참고자료13 문화일보, <"18회선 돌려쓰면 수만명 해킹" vs "장기 첩보戰선 불가능">

2015. 7. .

고발인들의 대리인
법무법인 이공
담당변호사 박 주 민

법무법인 동인
담당변호사 이 광 철

변호사 송 아 람

변호사 김 지 미

서울중앙지방검찰청 귀중