외교부 | 공동보도자료

보도시점 배포 즉시 보도 배포 2023. 6.2.(금) 06:00

북한 정권을 위해 정보·기술 탈취해 온 해킹조직 '김수키' 겨눈다

- 북한 해킹조직 '김수키'에 대한 한미 정부 합동 보안권고문 발표로 경각심 제고
- 우리 정부, 세계 최초로 '김수키'를 대북 독자제재 대상으로 지정
- '김수키', 인공위성·우주 개발 기술 탈취…북(北) 소위 '위성' 발사에 경고 조치

한미 양국은 6.2.(금) 대표적인 북한 해킹 조직으로서 전세계를 대상으로 정보·기술을 탈취해 온 '김수키(Kimsuky)'에 대한 한미 정부 합동 보안권고문을 발표하였다. 아울러, 우리 정부는 '김수키'를 세계 최초로 대북 독자제재 대상으로 지정하였다.

'김수키'는 외교·안보·국방 등 분야 개인·기관으로부터 첩보를 수집하여 이를 북한 정권에 제공해 왔다. 또한, '김수키'를 비롯한 북한 해킹조직들은 전세계를 대상으로 무기 개발 및 인공위성·우주 관련 첨단기술을 절취하여 북한의 소위 '위성' 개발에 직간접적인 관여를 해왔다.

이번 조치는 지난주 북한 정보기술(IT) 인력에 대한 한미 공동 독자제재(5.23) 후 10일 만에 이루어진 조치로, 북한 불법 사이버활동에 대한 한미 양국 정부의 단호하고 지속적인 대응 의지를 보여주는 것이다. 이번 조치가 '김수키'를 비롯한 북한 해킹 조직의 제반 활동에 대한 국내외 경각심을 제고하여 이들의 활동을 위축시키고, 북한의 해킹 공격으로부터 더욱 안전한 사이버 환경을 조성하는 데 기여할 것으로 기대한다.

또한, 이번 조치는 북한이 국제사회의 경고에도 불구하고 5.31(수) 소위 위성 명목의 장거리 탄도미사일을 발사한데 이어 재차 발사를 감행하겠다고 위협하고 있는 데 대응하여, 북한이 도발에 대한 대가를 반드시 치르도록 하겠다는 우리 정부의 강력한 의지를 보여주는 것이기도 하다.

【 김수키에 대한 한미 정부 합동 보안권고문 】

대한민국 국가정보원・경찰청・외교부와 미국 연방수사국(FBI)・국무부・국가안보국(NSA)은 북한 해킹조직 '김수키'의 해킹 수법을 상세히 알림으로써 이들의 활동에 대한 경각심을 제고하고, 피해가 발생하지 않도록 의심 활동에 대한 주의와 사이버 보안 조치를 강화할 것을 권고하는 한미 정부 합동 보안권고문을 발표하였다.

이번 권고문은 지난 2월 한미 정보당국이 발표한 '북한 금품 요구 악성 프로그램(랜섬웨어) 관련 한미 합동 사이버안보 권고'에 이어 한미 양국이 공동으로 발표하는 두 번째 권고문으로서, 그간 북한 불법 사이버 활동 대응을 위한 한미 간 긴밀한 공조를 반영한 것이다.

'김수키'는 정찰총국 산하 조직으로서 10여 년 동안 사이버 공격을 해왔다. 이들은 전 세계 정부・정치계・학계・언론계 주요 인사를 대상으로 사이버 공격을 감행하여 탈취한 외교 정책 등 정보를 북한 정권에 제공하고 있다.

'김수키'는 주로 사람의 신뢰・사회적 관계를 이용하여 사람을 속임으로써 비밀 정보를 획득하는 사회공학적 기법을 사용하여 사이버 공격을 감행하고 있다. 특히 표적 온라인 사기(스피어피싱) 공격*을 감행하여 정보를 탈취하고 있으며, 이번에 발표한 권고문에는 △'김수키'의 구체 활동 수법 △위험 지표(red flag indicators) △위협 완화 조치 등이 상세하게 기술되어 있다.

* 특정인을 속이기 위해 맞춤으로 제작된 이메일과 전자통신 내용을 활용하여 개인 정보를 훔치는 공격

이들은 △실제 언론사, 싱크탱크・대학, 정부기관・국회, 수사・법집행기관, 포털사이트 관리자 등 믿을만한 개인・단체를 사칭하면서 △외교・

안보 현안을 이용하여 △외교・통일・안보・국방・언론 분야 주요 인물에게 접근하며, △이메일에 첨부한 악성 프로그램을 통해 공격 대상의 계정, 기기, 컴퓨터 네트워크 등을 해킹하고 있다.

‘김수키’는 정교한 공격 수법을 사용하여 이들에 의해 자행되는 표적 온라인 사기(스피어피싱)공격을 식별하기 어렵게 만들고 있기 때문에 더욱 각별한 주의가 요구된다. 동 권고문은 △이메일 수신자들에 대해서는 출처가 확인되지 않은 이메일 등에 대한 주의 강화와 강력한 암호 설정・다단계 인증 등 계정 보호 조치를, △시스템 관리자들에 대해서는 서비스, 네트워크, 서버 등에 대한 보안 강화 조치들을 권고하고 있다.

북한 소행 표적 온라인 사기(스피어피싱) 공격의 대상이 되었다고 판단될 경우, 실제 침해가 발생했는지 여부와 관계없이 국정원(111), 경찰청(182), 한국인터넷진흥원(118) 등 소관기관에 신고할 것을 권고한다.

우리 정부는 앞으로도 미국 등 국제사회와의 협력과 민관 공조를 바탕으로, 북한의 불법 사이버활동에 대한 국내외 경각심을 높이기 위한 노력과 함께, 안전한 사이버 환경 조성을 위해 대국민 피해 예방 등 선제적 대응 활동을 적극 전개해 나갈 것이다.

【 우리 정부의 대북 독자제재 지정 】

우리 정부는 세계에서 최초로 ‘김수키’를 대북 독자제재 대상으로 지정하였다. 이번 제재는 윤석열 정부 출범 이후 8번째 대북 독자제재 조치로서, 우리 정부는 작년 10월 이후 개인 43명과 기관 45개를 독자제재 대상으로 지정하였다.

외교·안보 현안 등 비밀 정보 및 첨단기술 정보절취 등 ‘김수키’가 최근까지 국내 기관・개인을 대상으로 사이버 공격을 감행해 온 만큼, 이번 제재 조치를 통해 ‘김수키’의 국내 활동을 위축시키는 효과를 거둘 수 있을 것으로 기대한다. 또한, 김수키가 금품 요구 악성프로그램(랜섬웨어)* 공격을

감행하고 ‘몸값’을 요구해 오고 있는 상황에서 우리 정부가 자체 식별한 ‘김수키’의 가상자산 지갑 주소도 식별정보로 함께 등재함으로써 이들 활동에 대한 경각심을 제고하는 계기가 될 것으로 평가한다.

* 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 만든 뒤, 이를 인질로 금전(몸값)을 요구하는 악성 프로그램

이번 조치는 “외국환거래법”과 “공중 등 협박목적 및 대량살상무기확산을 위한 자금조달행위의 금지에 관한 법률”에 따른 것이다. 이번 금융제재 대상자로 지정된 대상과 외환거래 또는 금융거래를 하기 위해서는 각각 한국은행 총재 또는 금융위원회의 사전 허가가 필요하며, 허가를 받지 않고 거래하는 경우 관련법에 따라 처벌받을 수 있다. 아울러, 금융위원회의 사전 허가 없이 제재 대상으로 지정된 자와 가상자산을 거래하는 것도 금지된다.

※ “공중 등 협박목적 및 대량살상무기확산을 위한 자금조달행위의 금지에 관한 법률”상 ‘금융거래등’에 가상자산거래 포함

붙임 : 1. 북한 해킹조직 김수키에 대한 한미 정부 합동 보안권고문
2. 제재대상 식별 정보. 끝.

담당 부서	외교부 한반도평화교섭본부 북핵정책과	책임자	과 장	채경훈 (02-2100-8062)
		담당자	사무관	김지은 (02-2100-7878)
	경찰청 사이버수사국 사이버테러대응과	책임자	과 장	정석화 (02-3150-0053)
		담당자	경 정	이규봉 (02-3150-3071)
	기획재정부 국제금융국 외환제도과	책임자	과 장	이준범 (044-215-4750)
		담당자	사무관	임순묵 (044-215-4754)
	금융위원회 금융정보분석원 기획행정실	책임자	실 장	성기철 (02-2100-1720)
		담당자	사무관	김상협 (02-2100-1736)