과학기술정보통신부 보도자료 APEC 2025 KOREA

보도시점 2025. 11. 6.(목) 14:00 (2025. 11. 7.(금) 조간) 배포 2025. 11. 6.(목) 12:00

민관합동조사단, KT 침해사고 중간 조사결과 발표

- 소형 기지국(펨토셀)이 KT 망에 접속하는 과정에서 인증 관리에 문제가 있었음
- 단말-핵심망(코어망) 간 암호화 해제되어 불법 소형 기지국(불법 펨토셀)이 평문의 인증정보(자동응답체계<ARS>, 단문 메시지 서비스<SMS>)를 탈취한 것으로 판단
- KT는 '24.3~7월 기간 BPFDoor 등 악성코드 감염서버(43대)를 발견하였으나 정부에 신고하지 않았음
- 무단 소액결제 및 보안점검 과정에서 발견한 침해사고에 대해 지연 신고하였음

KT 침해사고 민관합동조사단(이하 "조사단")은 KT 침해사고에 대한 중간 조사결과를 11월 6일 발표하였다.

지난 9.8일, KT는 소액결제 피해자의 통화 이력을 분석한 결과 KT에 등록되지 않은 불법 기기가 내부망에 접속한 사실을 발견하여 한국인터넷진흥원(KISA)에 침해사고를 신고하였다. 과기정통부는 국민 금전 피해 발생 등 사고의 중대성, 공격 방식에 대한 면밀한 분석이 필요하다고 판단하여 9.9일부터 조사단을 구성•운영하고 있다.

조사단은 ▲불법 소형 기지국(불법 펨토셀)에 의한 소액결제 및 개인정보 유출사고, ▲국가배후 조직에 의한 KT 인증서 유출 정황(프랙보고서, 8.8), ▲KT가 외부업체를 통한 보안점검 과정에서 발견한 서버 침해사고 등 3건에 대한 조사를 통해 KT의 보안 문제점 등 사고 원인을 분석하였다.

< 불법 소형 기지국(불법 펨토셀)에 의한 소액결제 및 개인정보 유출사고 >

조사단은 불법 소형 기지국(불법 펨토셀)에 의한 소액결제 및 개인정보 유출사고와 관련하여 ①불법 소형 기지국(불법 펨토셀)으로 인한 피해 현황, ②KT의 소형 기지국(펨토셀) 관리 및 내부망 접속 인증 관련 문제점, ③소액결제 인증정보(자동응답체계<ARS>, 단문 메시지 서비스<SMS>) 탈취 각본(시나리오), ④과거 BPFDoor 등 악성코드 발견 및 조치 사실, ⑤침해사고 신고 지연 등 법령 위반 사항을 확인하였다.

조사단은 중간 조사결과에서는 KT의 일반적인 망 관리 실태 조사 및 시험 환경에서의 검증을 통해 소형 기지국(펨토셀) 운영 및 내부망 접속 과정 상의 보안 문제점을 도출하였으며, 최종적으로는 무단 소액결제 피의자로부터 확보한 불법 장비 분석을 통해 추가적인 보안 위협 요인을 파악하고 재발방지 대책을 마련하여 발표할 계획이다.

① 불법 소형 기지국(불법 펨토셀)로 인한 피해 현황

조사단은 이번 침해사고로 인한 피해자를 빠짐없이 파악하기 위해 KT에 피해 조사 대상 확대 및 분석방식 개선을 지속적으로 요구하였다. 이에 KT는 통신기록이 남아있는 '24.8.1.~'25.9.10 간 모든 기지국 접속 이력 약 4조 300억 건 및 모든 KT 가입자의 결제 약 1.5억 건 등 확보 가능한 모든 데이터를 분석하였으며, 이를 통해 불법 소형 기지국(불법 펨토셀) 20개에 접속한 22,227명의 가입자 식별번호(IMSI), 단말기 식별번호(IMEI) 및 전화번호 유출 정황이 확인되었으며, 368명, 2억 4,319만 원의 소액결제 피해를 발표(10.17)하였다.

다만, 통신기록이 없는 '24.8.1일 이전의 피해에 대해서는 파악이 불가능하였으며, 적은 수이긴 하지만 기지국 접속 이력이 남지 않은 소액결제 피해도 일부 있었다. 향후 조사단은 KT의 피해자 분석 방식 검증 및 누락된 피해자 존재 여부를 확인한 후 최종 피해 규모를 발표할 계획이다.

② KT의 소형 기지국(펨토셀) 관리 및 내부망 접속 인증 관련 문제점

조사단은 KT의 소형 기지국(펨토셀) 관리 체계가 전반적으로 부실하여 불법 소형 기지국(불법 펨토셀)이 KT 내부망에 쉽게 접속할 수 있는 환경이었음을 확인하였다. 먼저, KT에 납품되는 모든 소형 기지국(펨토셀)이 동일한 인증서를 사용하고 있어 해당 인증서를 복사하는 경우 불법 소형 기지국(불법 펨토셀)도 KT망에 접속이 가능함을 확인하였다. 또한, KT 인증서의 유효기간이 10년으로 설정되어 한 번이라도 KT망에 접속한 이력이 있는 소형 기지국(펨토셀)은 지속적으로 KT망에 접속할 수 있는 문제점을 발견하였다.

또한, 조사단은 소형 기지국(펨토셀) 제조사가 소형 기지국(펨토셀)에 탑재되는 셀 계정(셀ID), 인증서, KT 서버 인터넷 통신규약(IP) 등 중요정보를 보안관리 체계 없이 소형 기지국(펨토셀) 제작 외주사에 제공하였고, 소형 기지국(펨토셀) 저장 장치에서 해당 정보를 쉽게 확인 및 추출하는 것이 가능함을 확인하였다.

아울러 KT는 내부망에서의 소형 기지국(펨토셀) 접속 인증과정에서 타사 또는 해외 인터넷 통신 규약(IP) 등 비정상 인터넷 통신규약(IP)을 차단하지 않고 있었고, 소형 기지국(펨토셀) 제품 고유번호, 설치 지역정보 등 형상정보가 KT망에 등록된 정보인지 여부에 대해서도 검증하지 않았다.

조사단은 불법 소형기지국(불법 펨토셀) 접속 차단을 위해 통신3사의 신규 소형기지국 접속을 전면 제한(9.10)하는 한편, KT에 ▲소형기지국이 발급받은 통신사 인증서 유효기간 단축(10년 → 1개월, 9.10), ▲소형기지국이 KT 망에 접속 요구 시 KT 유선 인터넷 통신 규약(IP) 외에는 차단(9.23), ▲소형기지국이 KT 망에 접속 시 형상정보를 확인 및 인증(10.3~), ▲소형기지국 제품별 별도 인증서 발급(11.5) 등을 조치토록 하였다.

③ 소액결제 인증정보(자동응답체계<ARS>, 단문 메시지 서비스<SMS>) 탈취 각본(시나리오)

KT는 국제표준화기구(3GPP) 및 한국정보통신기술협회(TTA) 표준권고에 따라 단말과 기지국 간 구간 암호화와 단말과 핵심망(코어망) 간 종단 암호화를 하고 있다.

〈 통신사의 통신 암호화 체계 〉

□ 통신 3사는 국제표준화기구(3GPP) 표준 및 한국정보통신기술협회(TTA) 표준에 따라 암호체계 적용

- o (구간 암호화) 통신패킷이 흐르는 경로의 암호화로, 무선, 인터넷 구간에 암호화(통신사 국사 내 신뢰구간에는 암호화 미적용)
- o (종단 암호화) 단말에서 핵심망(코어망)까지 통신데이터 자체를 암호화하는 것으로, 문자 및 음성 시그널링*에 대해 국사 내 핵심망(코어망)까지 암호화

* 통화 시 상대방 식별, 세션 연결·해제 등을 관리하는 정보

조사단은 전문가 의견 청취, KT 통신망 시험대(테스트베드) 실험 등을 통해 불법 소형 기지국(불법 펨토셀)을 장악한 자가 종단 암호화를 해제할 수 있었고, 종단 암호화가 해제된 상태에서는 불법 소형 기지국(불법 펨토셀)이 인증정보(자동응답체계<ARS>, 단문 메시지 서비스<SMS>)를 평문으로 취득할 수 있었던 것으로 판단*하였다. 또한 불법 소형 기지국(불법 펨토셀)을 통해 결제 인증정보뿐만 아니라 문자, 음성통화 탈취가 가능한지에 대해서도 전문가 자문 및 추가 실험 등을 통해 조사해 나갈 계획이다.

* **판단근거**

- 전문가 의견 : 소형 기지국 하드웨어/소프트웨어(펨토셀 HW/SW) 자체 개발을 통해 전송되는 내용을 가로채는 기능 구현 가능
- 실험 결과 : 종단 암호화 해제 시 NW 구간에서 평문으로 데이터 전송되는 사실 확인

④ 과거 BPFDoor 등 악성코드 발견·조치 사실 확인

또한 조사단은 서버 디지털 증거 수집 및 분석(포렌식 분석) 등을 통해 과거 KT에 BPFDoor 등 악성코드 침해사고가 발생하였으며, KT가 이를 신고하지 않고* 자체 처리한 사실을 확인하였다. KT는 '24.3~7월의 기간 동안 BPFDoor, 웹셸 등 악성코드 감염서버(43대)를 발견하여 정부에 신고 없이 자체적으로 조치하고, 일부 감염 서버에서 성명, 전화번호, 이메일주소, 단말기 식별번호(IMEI) 등의 정보가 저장되어 있음을 조사단에 보고하였다. 조사단은 동 사안을 엄중히 보고 있으며, 사실관계를 면밀히 밝히고, 관계기관에 합당한 조치를 요청할 계획이다.

* 정보통신망법 상 3,000만 원 이하 과태료 부과 대상

⑤ 침해사고 신고 지연 사실 확인

KT는 ’25.9.1일에 경찰로부터 특정 지역의 무단 소액결제 발생을 전달받고, 내부망에 무단 소액결제 관련 이상 통신 호 유형(패턴)을 발견하여 차단 조치(9.5 03:00)하였음에도, 불법 소형기지국(불법 펨토셀) 계정(ID)의 존재를 확인한 후인 ’25.9.8(19:16)에 침해사고를 지연 신고*하였다.

* 정보통신망법 상 3,000만 원 이하 과태료 부과 대상

< 국가배후 조직에 의한 KT 인증서 유출 정황(프랙보고서, 8.8) 관련 >

프랙 보고서(8.8)에 언급된 국가배후 조직에 의한 KT 인증서 유출 정황과 관련하여 KT는 8.1일에 관련 서버를 폐기했다고 한국 인터넷진흥원에 답변하였으나, 실제로는 8.1(2대), 8.6(4대), 8.13(2대)에 걸쳐 폐기하는 등 폐기시점을 당국에 허위 제출하였다. 또한, KT는 폐기 서버 백업 기록(로그)이 있음에도 불구하고 9.18일까지 조사단에 이를 보고하지 않았다. 이에 조사단은 KT가 정부 조사를 방해하기 위한 고의성이 있다고 판단하여, 형법 제137조(위계에 의한 공무집행방해)에 따라 10.2일 수사기관에 수사 의뢰하였다.

< KT가 외부업체를 통한 보안점검에서 발견한 서버 침해사고 관련 >

KT는 외부 업체를 통한 보안점검 결과를 통해 ’25.9.15일 KT 내부 서버에 대한 침해 흔적이 있는 것을 확인하였으나, ’25.9.18일(23:57)에야 당국에 침해 사고를 지연 신고*하였다. 향후 침해 관련 서버에 대한 디지털 증거 복구 및 증거 분석(포렌식 분석)을 통해 사고 원인 및 KT의 보안 취약점을 도출할 계획이다.

* 정보통신망법 상 3,000만원 이하 과태료 부과 대상

조사단은 경찰과 협력하여 검거된 무단 소액결제 피의자로부터 압수한 불법 장비를 분석 중에 있으며, 개인정보위와 협력하여 무단 소액결제에 필요한 개인정보를 어떻게 확보하였는지 조사해 나갈 계획이다.

과기정통부는 KT 침해사고에 대한 엄정한 조사를 거쳐 최종 조사결과를 국민에게 투명하게 공개하는 한편, KT의 소형 기지국(펨토셀) 관리상 문제점, 과거 악성코드 발견 등 지금까지 확인된 사실관계 및 추후 밝혀질 조사결과를 토대로 법률검토를 거쳐 KT의 이용약관상 위약금 면제 사유에 해당하는지 여부를 발표할 계획이다.

담당 부서	과학기술정보통신부	책임자	과장	최광기 (044-202-6460)
	사이버침해대응과	담당자	사무관	김성환 (044-202-6461)
	과학기술정보통신부	책임자	과장	김준모 (044-202-6650)
	통신이용제도과	담당자	사무관	구희선 (044-202-6655)
관련 기관	한국인터넷진흥원	책임자	단장	박용규 (02-405-4800)
	위협분석단	담당자	팀장	김홍석 (02-405-4830)