

[단독]北추정 해커, 정부문서시스템 개발업체 자료 대거 해킹 | 동아일보

donga.com/news/Society/article/all/20250212/131012660/2

February 12, 2025

정치부에서 국방부를 출입하고 있습니다.

부처 문서 공유-결재 통합 '온-나라'
영상회의-국무회의 자료 등도 등록
“해킹 취약점 노출 땀 보안에 치명적”



그래픽 김민호 기자

©뉴스시스

북한으로 추정되는 해킹 세력이 범정부 전자문서관리시스템인 '온-나라'의 개발업체를 해킹해 정보 당국이 조사 중인 것으로 확인됐다. 온-나라는 전 정부부처에서 문서 작성 및 검토, 결재 등 공문서를 처리할 때 사용하는 통합 프로그램으로 개발·구축·운영을 맡은 업체 서버에서 관련 자료가 대거 탈취된 것으로 전해졌다. 이번 해킹 공격으로 온-나라 프로그램 구조는 물론이고 해킹 취약점이 고스란히 북한에 노출된 것 아니냐는 우려가 나온다.

11일 동아일보 취재를 종합하면 당국은 지난해 말 온-나라 개발업체인 A 업체에 대한 해킹 피해를 인지해 피해 규모 등의 조사에 나섰다. 당국은 해킹을 북한의 소행으로 보고 있는 것으로 전해졌다. 국가정보원은 “현재 조사 중인 사안으로 (세부 내용은) 확인이 어렵다”고 밝혔다.

A 업체는 온-나라 개발 및 구축, 운영 등을 담당하는 전문 업체다. 2005년 구축된 온-나라는 2010년대 후반 기관별로 운영되던 전산 환경을 업무 효율화를 위해 ‘클라우드’로 통합해 부처간 공동작업 등이 가능하도록 개선됐다. 정부 내부망에 전 부처들끼리 문서를 공유하고 결재를 할 수 있는 통합 시스템이 구축돼 있는 것. 문서 결재뿐만 아니라 메일, 영상회의를 비롯해 국무회의 자료나 부처 일정 등도 등록된다.

북한은 여러 단계를 거쳐 목표에 접근해 가는 침투 전략으로 온-나라 프로그램의 구조나 구축 당시 사용된 프로그램, 부처 내부 문서 등을 A 업체 해킹을 통해 파악한 것으로 보인다. 특히 이번 해킹을 통해 취약점을 파악한 뒤 향후 정부망에 대한 직접적인 해킹을 시도해 정부 행정망을 마비시키고 민감 문서 등의 탈취를 시도할 수 있다는 점에서 사이버 보안에 치명적일 수 있다는 지적이 나온다. 당국은 2023년 말부터 이어진 김정은 국무위원장의 ‘적대적 두 국가론’ 기조에서 향후 우리 정부를 흔들기 위한 해킹 공격을 강화할 것으로 보고 있다.

실제 북한은 이번 해킹과 유사하게 정부나 대기업을 대상으로 한 직접 침투 대신 보안이 상대적으로 취약한 민간 중소기업체를 ‘핀포인트’해 우회 해킹하는 방식으로 정보 탈취에 주력하는 동향을 보이고 있다. 지난해 대형 방산기업의 협력업체가 해킹당해 우리 군 핵심 대북 공중정찰 자산인 백두·금강 정찰기 관련 자료들이 상당수 유출됐고, 장갑차·미사일·레이더 등 주요 무기체계 핵심 부품을 생산하는 협력업체의 기술 상당수도 탈취됐다. 특히 김 위원장의 관심사에 따라 여러 해킹 조직이 빠르게 대상을 바꿔 가며 동시에 공격을 감행하고 있다고 한다.

동아일보 단독 >



- **“집값 영향” 공개 안한 서울시 ‘싱크홀 지도’... 지질조사도 안했다**
- **‘싱크홀 지도’ 만든다더니, 지질조사도 안했다**
- **대통령실 파견 국힘 당직자 10여명 내주 복귀**

이런 구독물도 추천합니다!



•

정치를 부탁해

구독



•

이은화의 미술시간

구독



•

형설수설

구독

#은-나라#북한#해킹
신규진 기자 newjin@donga.com

- 좋아요
0개
- 슬퍼요
0개
- 화나요
0개

댓글 0

지금 뜨는 뉴스



끊이지 않는 '투표지 분류기 조작설'... “민관정 검증단 꾸려 감시를”



[횡설수설/우경입]차기 주자들 너도나도 “용산 안 간다”



[사설]헌법재판관 '임명'조차 거부하던 韓대행은 왜 표변했을까

- 좋아요

0개

- 슬퍼요

0개

- 화나요

0개

-

트렌드뉴스

-

-

댓글 0

© dongA.com All rights reserved.

© dongA.com All rights reserved.