North Korean hackers breach South Korea's atomic research agency through VPN bug

By Catalin Cimpanu

Published: 2022-12-16 · Archived: 2026-04-05 18:02:16 UTC

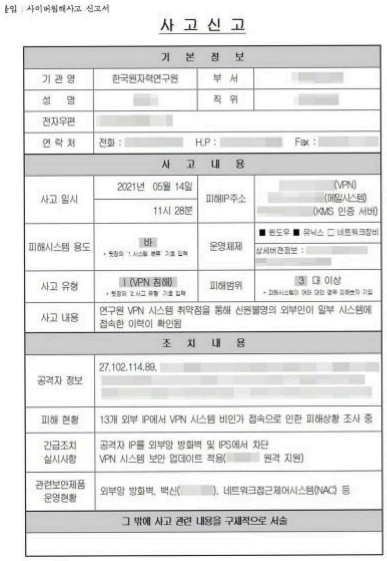
South Korean officials said on Friday that hackers believed to be operating out of North Korea breached the internal network of the South Korean Atomic Energy Research Institute (KAERI), the government organization that conducts research on nuclear power and nuclear fuel technology.

In a press conference, a KAERI spokesperson said the intrusion took place last month on May 14, through a vulnerability in a virtual private network (VPN) server.

Thirteen different IPs were seen abusing the vulnerability and accessing the organization's internal network.

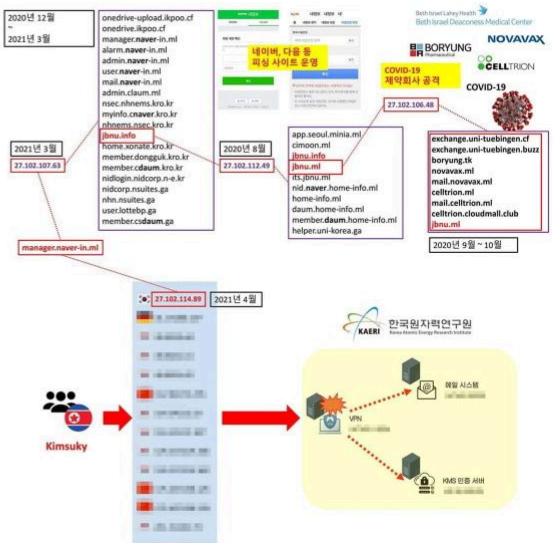
One of these IP addresses was linked to attack infrastructure used by Kimsuky, a North Korean cyber-espionage group.

The name of the VPN server vendor was redacted in documents presented to South Korean press today at a KAERI press conference.



사 고 신 고

가 본 정 보			
기 관 명	한국원자력연구원	부 서	
성 명		직 위	
전자우편			
연 락 처	전화 :	H.P :	Fax :
사 고 내 용			
사고 일시	2021년 05월 14일 11시 28분	피해IP주소	(VPN) (메일시스템) (KMS 인증 서버)
피해시스템 용도	비	운영체제	■ 윈도우 ■ 유닉스 □ 네트워크장비
사고 유형	1 (VPN 점해)	피해범위	3 대 이상
사고 내용	연구원 VPN 시스템 취약점을 통해 신원불명의 외부인이 일부 시스템에 접속한 이력이 확인됨		
조 치 내 용			
공격자 정보	27.102.114.89,		
피해 현황	13개 외부 IP에서 VPN 시스템 비인가 접속으로 인한 피해상황 조사 중		
긴급조치 실시사항	공격자 IP를 외부망 방화벽 및 IPS에서 차단 VPN 시스템 보안 업데이트 적용(원격 지원)		
관련보안제품 운영현황	외부망 방화벽, 백신( ), 네트워크접근제어시스템(NAC) 등		
그 밖에 사고 관련 내용을 구체적으로 서술			



KAERI held a press conference today after news of the hack leaked to reporters earlier this month, and the agency came under criticism for initially denying the intrusion.

In a press release posted on its website after the press conference, the agency apologized for its initial denial.

News of Kimsuky's KAERI hack comes after security firm Malwarebytes published a report at the start of the month exposing a Kimsuky spear-phishing campaign that targeted several South Korean government entities, but

also the nuclear security officer for the International Atomic Energy Agency (IAEA), a UN organization tasked with nuclear regulations and cooperation.

All North Korean cyber-espionage groups, not just Kimsuky, have all been historically interested in nuclear energy and nuclear arms-related targets, primarily due to the country's controversial nuclear weapons program.

In September 2019, the US Treasury Department sanctioned three North Korean hacking groups (Lazarus, Andariel, Bluenoroff) for hacks aimed at stealing funds to funnel back into the country's nuclear weapons and missile programs.
