경찰청 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2024. 4. 24.(수) 조간 누리망 · 방송 2024. 4. 23.(화) 12:00

경찰청·방위사업청 등 관계기관 합동 특별점검을 통해 북한의 케이(K)-방산업체 해킹 공격 규명 및 보호조치 실시

- 북 해킹조직 라자루스·안다리엘·김수키 모두 방산기술 노려
- 방산업체 등에 “전자우편 비밀번호 주기적 변경, 미인가 아이피(IP) 접속 차단 등 보안 조치 강화” 당부

경찰청 국가수사본부(안보수사국)는 국가사이버위기관리단과 공조해 국내 방산기술 유출 사건을 수사한 결과, 라자루스·안다리엘·김수키 등으로 알려진 북한 해킹조직들이 국내 방산기술 탈취하기 위해 전방위적으로 공격하고 있는 것을 확인하고 보안 조치를 취했다.

북한 해킹조직은 방산업체를 직접 침투하기도 하고, 상대적으로 보안이 취약한 방산 협력업체를 해킹하여 방산 업체의 서버 계정정보를 탈취한 후 주요 서버에 무단으로 침투해 악성코드를 유포한 것으로 파악되었다.

□ 수사 경과

이번 사건은 경찰청이 국가사이버위기관리단 등 관계기관과 사이버 위협 정보 공유를 통해 공격 수법 등을 확인하였으며, 경찰청은 ▵공격에 사용한 아이피(IP) 주소 ▵경유지 구축 방법 ▵공격에 사용한 악성코드 등을 근거로 이번 사건을 북한 해킹조직의 소행으로 판단하였다.

경찰청은 방위사업청 등 관계기관 합동으로 특별점검*을 실시하여 피해 보호조치를 병행하였고, 특별점검 과정에서 일부 피해업체들은 경찰의 연락을 받기 전까지도 해킹 피해 사실을 전혀 모르고 있었다.

* 합동 점검: 2024. 1. 15.(월)~2. 16.(금) 경찰청, 방사청, 국정원 등으로 구성/점검

이번 사건을 통해 북한 해킹조직이 방산기술 탈취라는 공동의 목표를 설정하여 다수의 해킹조직을 투입하는 총력전 형태로 공격을 진행하는 등 공격 수법은 더욱 치밀하고 다양하게 진행하고 있는 것으로 확인되었다.

□ 사례별 공격특징

○ 사례 1 (라자루스 해킹조직)

피해업체가 내부망과 외부 인터넷망을 분리 운영하였지만, 망 연계 시스템의 관리 소홀을 틈타 내부망으로 침입한 사례이다.

북한 해킹조직은 2022년 11월부터 '가' 방산업체 외부망 서버를 해킹하여 악성코드에 감염시킨 후 테스트 목적으로 열려있는 망 연계 시스템의 포트를 통해 회사 내부망까지 장악하였다. 개발팀 직원 컴퓨터 등 내부망의 중요자료를 수집하여 국외 클라우드 서버로 자료를 빼돌렸다.

내부망 컴퓨터 6대에서 자료가 유출된 사실이 확인되었는데, 피해업체와 국외 클라우드 서버 등 분석을 통해 유출된 자료의 흔적을 확인할 수 있었다.

○ 사례 2 (안다리엘 해킹조직)

방산 협력업체의 서버를 유지 보수하는 업체 직원이 사용하는 계정을 탈취하여 악성코드를 감염시켜 방산 자료를 유출한 사례이다.

북한 해킹조직은 2022년 10월경부터 '나' 방산 협력업체 등을 원격으로 유지 보수하는 '다' 업체의 계정정보를 탈취하여 '나' 방산 협력업체 등에 악성코드를 설치하였고 이 과정에서 감염된 서버에 저장된 방산기술 자료가 유출되었다.

이는 '다' 업체 직원의 개인 상용 전자우편(네이버 · 카카오 등) 계정정보를 탈취하고 사내 전자우편으로 접속하여 전자우편 송수신 자료를 탈취한 것으로, 일부 직원들이 상용 전자우편 계정과 사내 업무시스템 계정(아이디와 비밀번호)을 같이 사용하는 허점을 악용하였다.

○ 사례 3 (김수키 해킹조직)

사내에서 사용하는 그룹웨어 전자우편서버의 취약점(로그인 없이 외부에서 전자우편으로 송수신한 대용량 파일을 다운로드 가능)을 악용한 사례이다.

북한 해킹조직은 2023년 4월부터 7월까지 '라' 방산 협력업체 전자우편 서버에서 로그인 없이 외부에서 전자우편으로 송수신한 대용량 파일을 다운로드 가능한 취약점을 악용하여 피해업체의 기술자료를 탈취하였다.

□ 피해 예방 및 향후 계획

경찰청은 "방산기술을 대상으로 한 북한의 해킹 시도가 지속해서 이어질 것으로 전망되니 방산업체 뿐만 아니라 협력업체에 대해서도 내외부망 분리, 전자우편 비밀번호의 주기적인 변경과 2단계 인증 등 계정 인증 설정, 인가되지 않은 아이피(IP) 및 불필요한 해외 아이피(IP) 접속 차단 등의 보안 조치를 강화해 달라"라고 당부하였다.

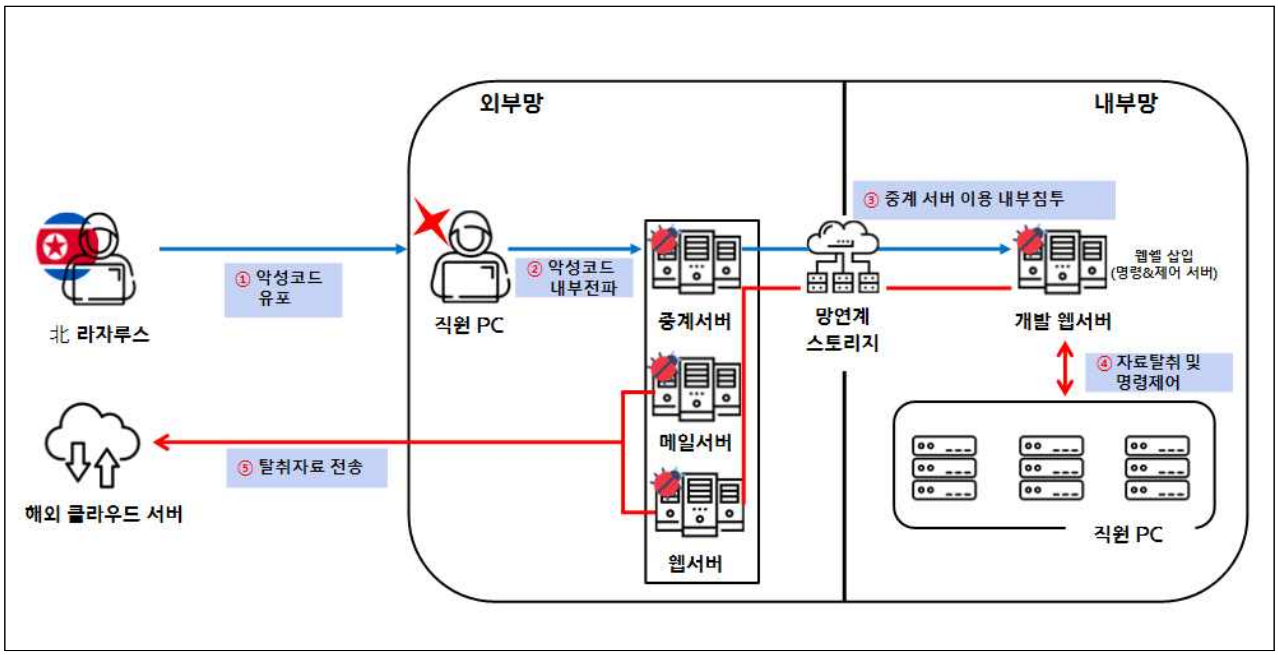
아울러, "경찰청은 앞으로도 북한 등 국가배후 해킹조직의 추적 수사를 지속하는 한편, 사이버 공격 동향과 대응 사례를 방위사업청, 국가사이버위기관리단 등 관계기관과 적극적으로 공유해 국가안보의 위협에 선제적으로 대응할 예정이다."라고 밝혔다.

붙임: 사례별 사건 개요도

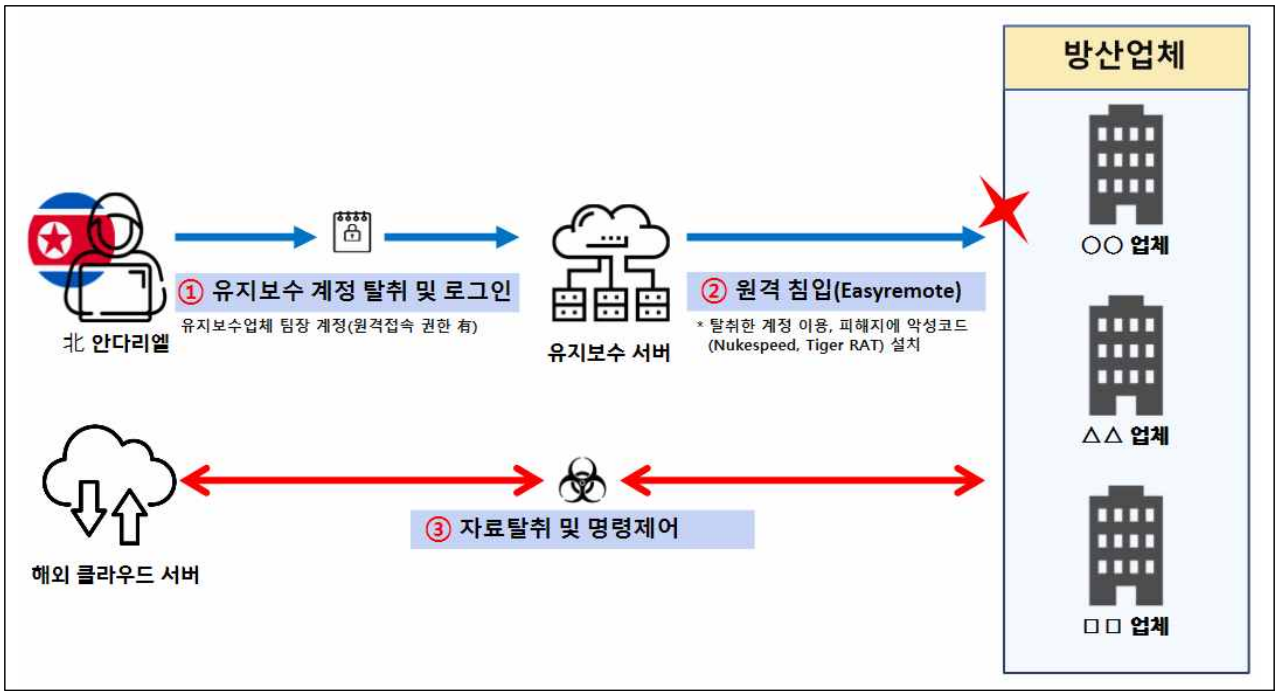
담당 부서	국가수사본부 안보수사국 안보수사지휘과	책임자	총경	김산호 (02-3150-2092)
		담당자	경정	권대홍 (02-3150-2492)

붙임	사례별 사건 개요도

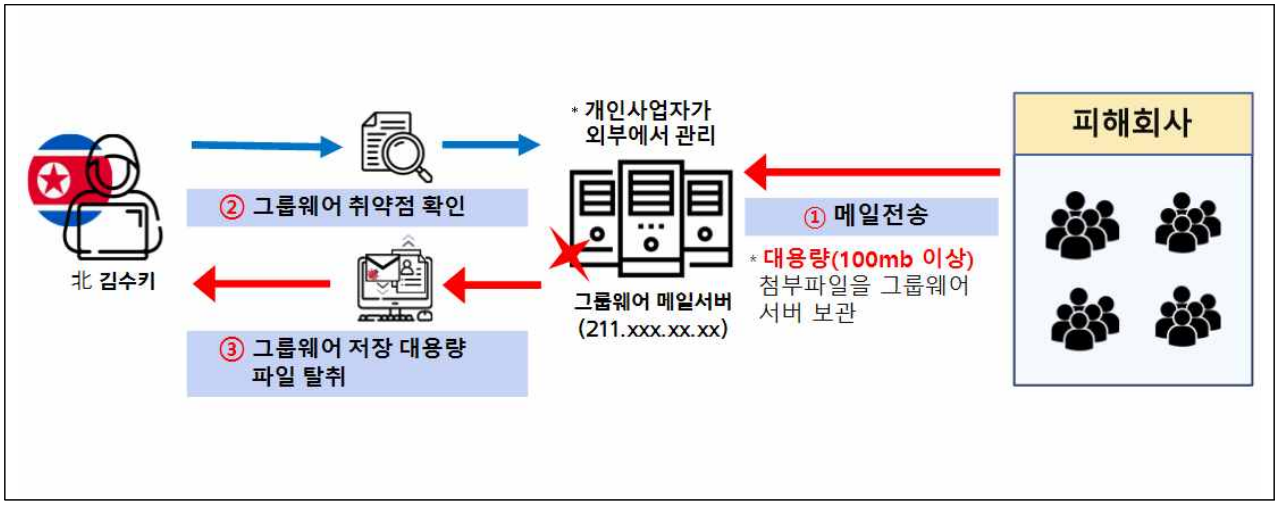
○ 사례 1 (라자루스 해킹조직)



○ 사례 2 (안다리엘 해킹조직)



○ 사례 3 (김수키 해킹조직)


北 김수키
② 그룹웨어 취약점 확인
③ 그룹웨어 저장 대용량 파일 탈취
* 개인사업자가 외부에서 관리
그룹웨어 메일서버 (211.xxx.xx.xx)
① 메일전송
* 대용량(100mb 이상) 첨부파일을 그룹웨어 서버 보관
피해회사