금융미래를 열어가는 금융보안파트너

금융보안원 FINANCIAL SECURITY INSTITUTE	보 도 자 료 배포시부터 보도 가능	배 포 일 2025. 3. 13.

작성부서	침해대응부 침해위협분석팀		
책 임 자	팀장 송아현 (02-3495-9420)	담 당 자	수석 강대규 (02-3495-9422) 책임 장성욱 (02-3495-9423)

제목 : 금융보안원, 국가배후 해킹조직의 금융권 대상 위협 경고

◇ 금융당국이 발송한 가상자산 관련 문서로 위장한 악성코드가 지속적으로 발견되고 있어 각별한 주의 필요

□ **금융보안원(원장 박상원)**은 개인·금융정보를 노리는 **국가배후 해킹조직의 악성코드 위협이 지속**되고 있다고 밝히며 **금융회사 및 금융소비자의 각별한 주의를 당부**

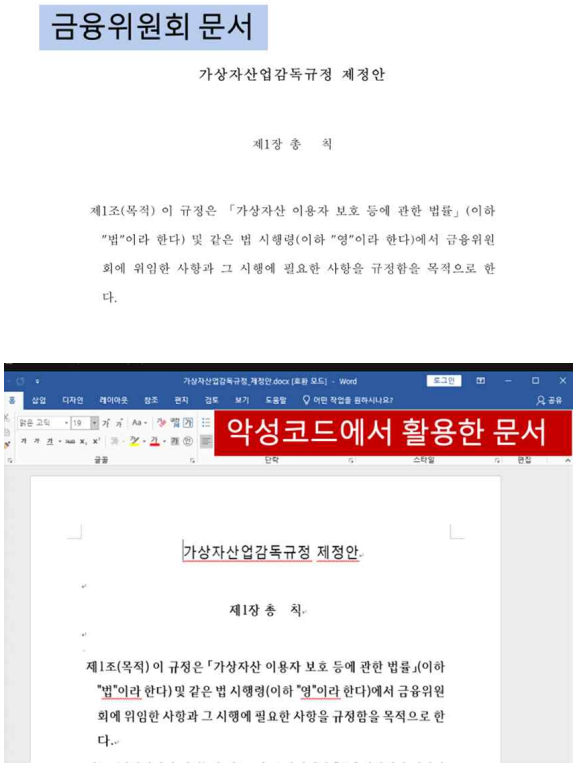
○ 특히, 가상자산에 대한 사회적 관심이 높아지고 있는 상황에서 **금융당국의 가상자산 관련** 문서로 **위장한 악성코드**를 이용해 **가상자산에 관심** 있는 **금융소비자의 정보를 탈취**하고 **단말기를 장악**하거나 가상자산거래소 직원을 표적으로 하는 등 **가상자산 관련 정교한 공격**이 지속적으로 발견

□ 국가배후 해킹조직은 가상자산 뿐만 아니라 금융산업을 포함한 **다양한 분야를 대상**으로 **공격 범위를 확장**하고 있으며 **공격 대상에 특화된 지능적·표적화 침투 기법**을 활용

※ [첨부] 국가배후 해킹조직의 주요 공격 및 특징

□ 국가배후 해킹조직은 **금융당국의 가상자산 관련 문서로 위장한 바로가기(.LNK) 파일** 또는 **공격 스크립트가 담긴 문서 파일**이 첨부된 **피싱메일을 발송**하여 **악성코드 설치를 유도**

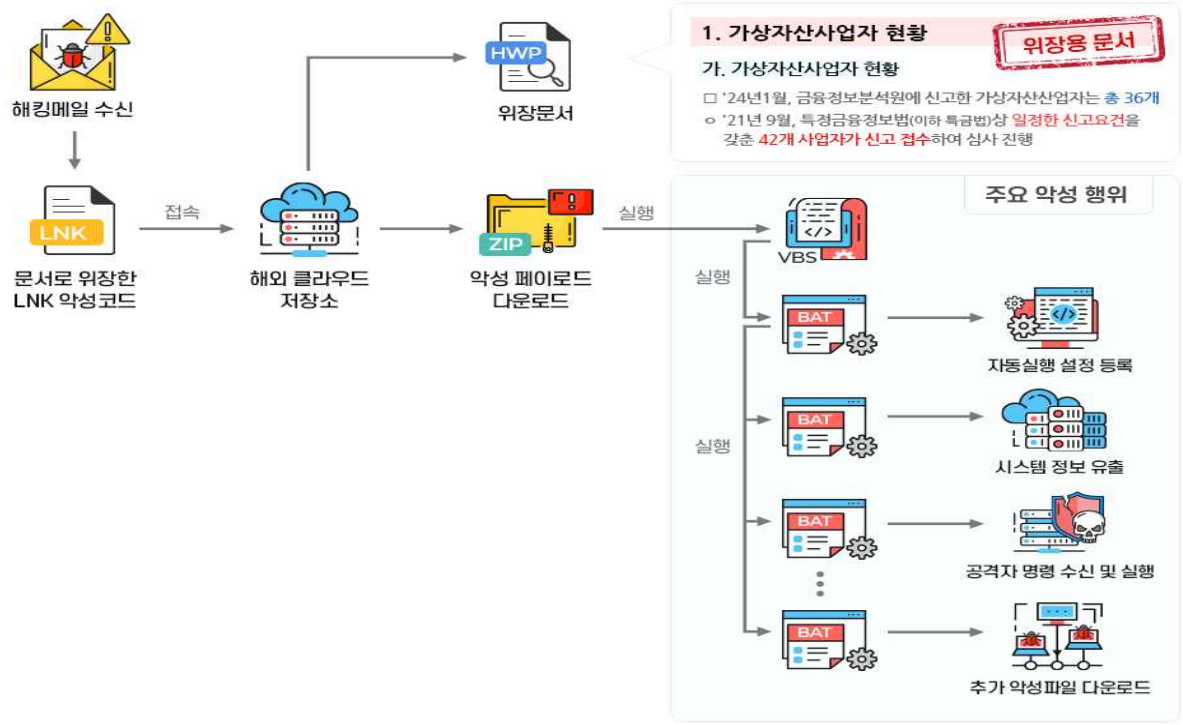
<정부 사칭 피싱메일 및 미끼문서 예시>



○ 설치된 악성코드는 **미끼 문서를 출력하여 피해자의 의심을 회피**하는 동시에 **클라우드 저장소로 사용자 정보를 유출**하고, **원격 제어 도구 등을 설치**하여 지속적인 악성행위를 수행

○ 이는 **지속적 정보 수집 및 표적 네트워크의 감시**를 통한 기밀 탈취, 자금 확보 및 사이버 첩보 활동 등 전략적 이익 강화가 목적으로 보임

<국가배후 해킹조직의 악성코드 공격 흐름>



□ **금융보안원**은 **금융권을 표적으로 하는 침해위협** 및 **악성코드**를 **수집·분석**하고 그 결과를 **금융회사 및 유관기관에 신속히 공유**함으로써 **피해 예방에 만전을** 기하고 있음

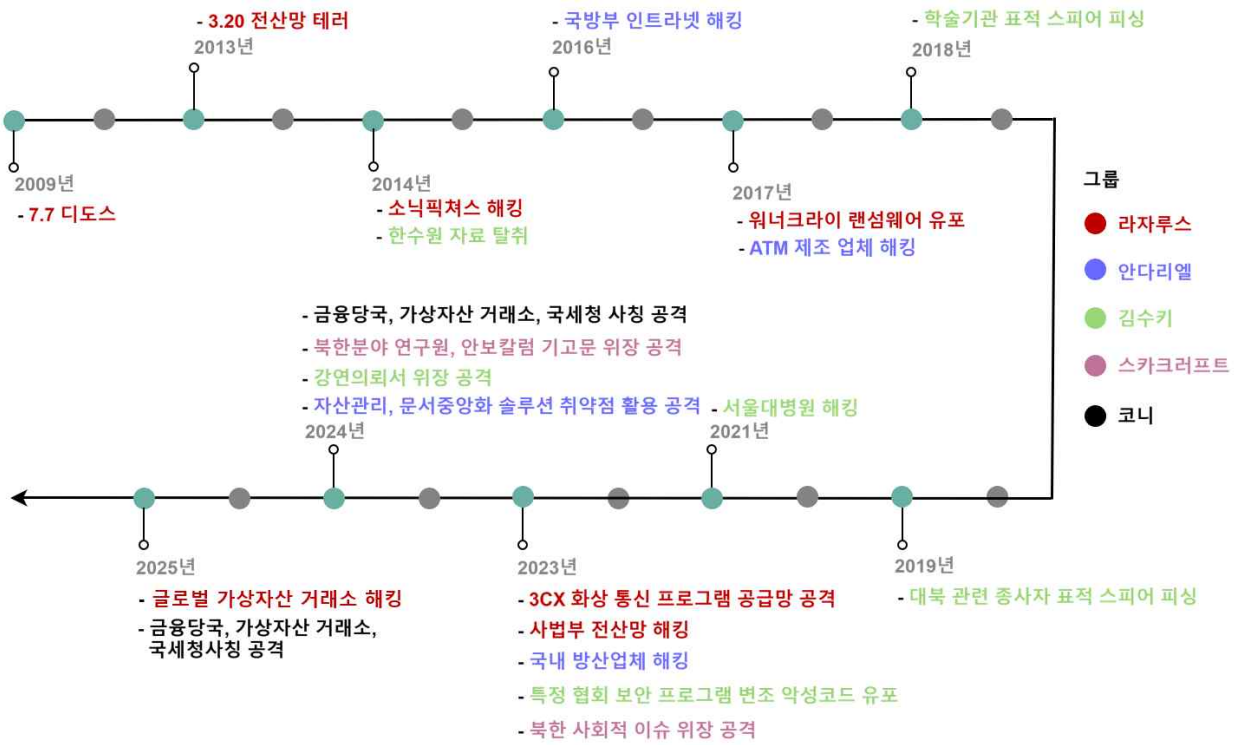
○ **금융소비자**는 **출처가 불분명한 이메일 열람 및 첨부파일 실행을 삼가고** 정부기관이나 **금융회사를 사칭한 메시지에 주의**하는 등 **기본적인 보안수칙을 생활화**하는 것이 중요

○ 또한, 가상자산거래소는 국가배후 해킹조직의 **가상자산 탈취 등 위협이 증가**하고 있어 **안전성 및 보안성을 강화**할 필요

□ **금융보안원 박상원 원장**은 "나날이 정교해지는 **국가배후 해킹조직의 표적 공격에 대처**하기 위해서는 **금융권의 침해위협 분석 대응 역량을 한층 강화해야 한다**"면서,

○ "금융보안원은 **생성형 AI를 활용**해 **금융권 위협을 분석하고 해킹조직의 공격전술 및 악성코드 패턴을 연관 분석**하는 등 **변화하는** 사이버 **위협에 철저히 대비**해 나가겠다"고 밝힘. 끝.

첨부 국가배후 해킹조직의 주요 공격 및 특징



해킹조직 (등장시기)	공격 사례	공격 특징
라자루스 (2009)	■ 7.7 디도스('09), 3.20 전산망 테러('13) ■ 워너크라이 랜섬웨어 유포('17) ■ 사법부 전산망 해킹('23) ■ IT개발자 위장취업 및 오픈소스 공급망 공격('24) ■ 글로벌 가상자산거래소 해킹('25) 등	■ 경제적 이익 및 정보 탈취 ■ 악성코드 유포를 위해 오픈소스 공급망 활용 등
김수키 (2012)	■ 한국수력원자력 해킹('14) ■ 학술기관, 대북관련 종사자 스피어피싱('18) ■ 특정 협회 보안 프로그램 변조 악성코드 유포('23) 등	■ 한글(HWP)문서를 활용한 스피어피싱 ■ 외교 및 통일분야 관련 위장 문서 활용 등
스카크러프트 (2012)	■ 안보칼럼 사칭 악성코드 유포('24) ■ 북한 분야 연구원 위장 해킹메일 유포('24) 등	■ 국내외 정치·사회 이슈를 활용한 스피어피싱 ■ 시스템 장악 및 정보유출 등
안다리엘 (2014)	■ 국방부 인트라넷 해킹('16) ■ 국내 방산업체 해킹('23) 등	■ 국내 관리 솔루션 등 취약점 악용
코니 (2017)	■ 가상자산거래소 사칭 악성코드 유포('24) ■ 국세청 사칭 악성코드 유포('24) 등	■ 금융관련 문서 및 금융 당국 사칭 등