2023년 1차

사이버보안 대연합 보고서

탐지·공유 분과

1. 2023년 6월 글로벌 해킹그룹 동향 분석 [장영준 수석, NSHC]
2. 한국 내 대북분야 종사자 겨냥 BitB 공격 동향 분석 [문종현 이사(센터장), 지니언스 시큐리티 센터(GSC)]

KISA 한국인터넷진흥원

kisia 한국정보보호산업협회

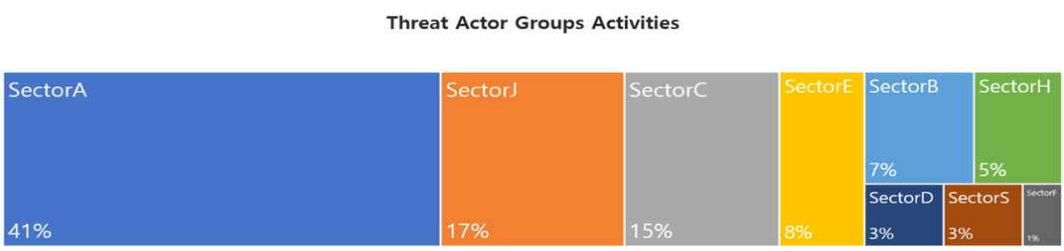
2023년 6월 글로벌 해킹그룹 동향 분석

장영준 수석, NSHC, cyj@nshc.net

1. 개요

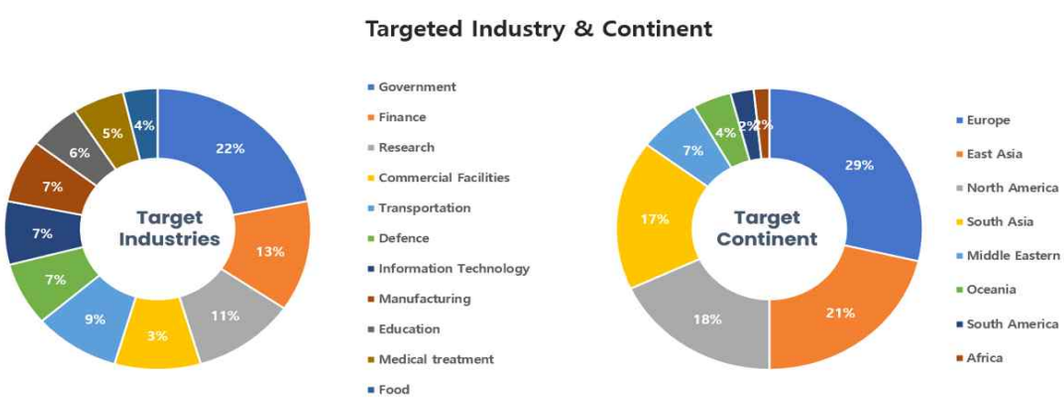
2023년 5월 21일에서 2023년 6월 20일까지 NSHC ThreatRecon팀에서 수집한 데이터와 정보를 바탕으로 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다. 이번 6월에는 총 32개의 해킹 그룹들의 활동이 확인되었으며, SectorA 그룹이 41%로 가장 많았으며, SectorJ 그룹의 활동이 그 뒤를 이었다.

[그림 1] 2023년 6월에 확인된 해킹 그룹별 활동 통계



이번 6월에 발견된 해킹 그룹들의 해킹 활동은 정부기관과 금융 분야에 종사하는 관계자 또는 시스템들을 대상으로 가장 많은 공격을 수행했으며, 지역별로는 유럽(Europe)과 동아시아(East Asia)에 위치한 국가들을 대상으로 한 해킹 활동이 가장 많은 것으로 확인된다.

[그림 2] 2023년 6월 공격 대상이 된 산업 분야와 국가 통계



2. 해킹그룹별 활동 특징

1) SectorA 그룹 활동 특징

SectorA 그룹들 중 이번 6월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA01, SectorA02, SectorA05, SectorA06, SectorA07 그룹이다.

SectorA01 그룹은 한국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 한국에서 사용하는 웹 보안 프로그램과 기업 자산 관리 프로그램의 원격 코드 실행(Remote Code Execution) 취약점을 사용하여, 공격 대상 시스템에서 악성코드를 다운로드 및 실행했다.

SectorA02 그룹은 한국, 호주, 캄보디아, 미국, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 윈도우 바로가기(LNK) 파일 형식의 악성코드를 사용했으며, 북한인권 영화 상영회 협조 요청 문서로 위장하여 공격 대상이 악성코드를 실행하도록 유도했다.

SectorA05 그룹은 한국, 벨기에, 미국, 중국, 일본, 우크라이나, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 북한 인권 단체와 관련된 주제로 위장한 피싱(Phishing) 메일에 윈도우 도움말 (CHM, Compiled HTML Help) 파일 형식의 악성코드가 존재하는 압축파일을 첨부하여 공격 대상에게 전달했으며, 최종적으로 시스템의 다양한 정보를 유출하는 악성코드를 사용했다.

SectorA06 그룹은 아랍에미리트, 호주, 이스라엘, 스위스, 인도네시아, 인도, 미국, 루마니아, 중국, 일본, 싱가포르, 미국, 이탈리아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 맥OS(macOS) 사용자를 대상으로 PDF 뷰어(PDF Viewer)로 위장한 악성코드를 사용했으며, 공격 대상을 속이기 위해 마이크로소프트 애저(Microsoft Azure)의 보호된 문서로 위장한 미끼 문서를 사용했다.

SectorA07 그룹은 한국, 이스라엘에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 감정평가 협조 안내문으로 위장한 윈도우 바로가기(LNK) 형식의 악성코드를 ZIP 파일 형식으로 압축 후 배포했으며, 최종적으로 시스템 정보를 수집하는 비주얼 베이직 스크립트(Visual Basic Script)와 배치(Batch) 스크립트 파일을 사용했다.

현재까지 계속 지속되는 SectorA 해킹 그룹들은 한국과 관련된 정치, 외교 활동 등 정부 활동과 관련된 고급 정보를 수집하기 위한 목적을 가지며 전 세계를 대상으로 한 금전적인 재화의 확보를 위한 해킹 활동을 병행하고 있다. 이들의 해킹 목적은 장기간에 걸쳐 지속되고 있으며, 이러한 전략적 해킹 목적으로 당분간 변화 없이 지속적으로 진행될 것으로 판단된다.

2) SectorB 그룹 활동 특징

SectorB 그룹들 중 이번 6월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB22, SectorB38, SectorB50, SectorB73, SectorB75 그룹이다.

SectorB22 그룹은 라트비아, 타이완, 미얀마, 일본, 터키, 에스토니아, 그리스, 영국, 미국, 핀란드, 독일, 노르웨이에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 및 기관, 통신 산업 등의 다양한 조직을 대상으로 스피어 피싱(Spear Phishing) 이메일을 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 시스템 정보 수집, 명령 실행, 파일 삭제 등의 악성 행위를 수행하였다.

SectorB38 그룹은 미국, 이탈리아, 캐나다, 인도, 오스트레일리아, 싱가포르, 프랑스, 독일, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 및 기관, 외교부, 금융 등의 다양한 조직을 대상으로 스피어 피싱 이메일을 배포하여 공격 활동을 하였으며, 공격 대상 시스템에서 다운로더(Downloader) 기능의 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

SectorB50 그룹은 아랍에미리트, 미국, 독일에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 설문조사 문서로 위장한 압축 파일을 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 공격자의 명령에 따른 악의적인 행위를 수행하게 된다.

SectorB73 그룹은 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 중요 인프라 제공업체를 대상으로 공격 활동을 하였으며, 다양한 오픈 소스(Open Source) 도구 및 시스템 명령을 활용하여 정보 탈취 행위를 하였다.

SectorB75 그룹은 라트비아, 파키스탄, 중국, 독일, 홍콩, 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 바라쿠다 이메일 시큐리티 게이트웨이 어플라이언스(Barracuda Email Security Gateway Appliance) 장비에서 발생한 취약점(CVE-2023-2868)을 악용하여 공격 활동을 하였으며, 공격 대상 시스템에서 정보 탈취 행위를 하였다.

현재까지 지속되는 SectorB 해킹 그룹들의 해킹 활동 목적은 전 세계를 대상으로 각국 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 것으로 분석된다.

3) SectorC 그룹 활동 특징

SectorC 그룹들 중 이번 6월 총 6개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorC01, SectorC04, SectorC05, SectorC08, SectorC13, SectorC14 그룹이다.

SectorC01 그룹의 활동은 우크라이나에서 발견되었다. 해당 그룹은 웹 메일 소프트웨어의 취약점을 악용하여 웹 메일 서버의 정보를 탈취했으며, 송수신 메일 주소를 변조하거나, 사용자 주소록을 훔쳐 2차 공격을 위한 발판을 마련했다.

SectorC04 그룹은 마이크로소프트 인증서로 서명된 정상적인 EXE 파일을 DLL 사이드 로딩(Side-Loading) 기법에 사용하여 악성코드를 실행시켰으며, 최종적으로 추가 악성코드를 다운로드 및 실행할 수 있는 다운로더(Downloader) 기능의 악성코드를 사용했다.

SectorC05 그룹의 활동은 우크라이나에서 발견되었다. 해당 그룹은 다단계 인증(MFA)이 없는 VPN 계정을 악용하였으며, 시스템 파괴 목적을 가진 배치(Batch) 스크립트 형식의 악성코드를 사용하여 시스템 내에 파일들을 삭제했다.

SectorC08 그룹의 활동은 미국, 러시아, 아랍에미리트, 우크라이나, 폴란드, 한국에서 발견되었다. 해당 그룹은 망 분리(Air Gap)가 된 시스템에 도달하기 위해 이동식 매체를 이용하여 측면 이동(Lateral Movement)을 시도했으며, 공격 대상 조직의 시스템에 윈도우 바로가기(LNK) 형식의 악성코드를 생성하여 공격 대상이 실행하도록 유도하는 방식을 사용했다.

SectorC13 그룹의 활동은 미국, 러시아에서 발견되었다. 해당 그룹은 포격에 대한 대피행동요령에 대한 내용으로 위장한 MS 워드(Word) 악성코드를 사용했으며, 공격 대상이 MS 워드(Word) 악성코드를 실행할 경우 템플릿 인젝션(Template Injection) 기법을 통해 악의적인 코드가 포함된 MS 워드(Word) 템플릿(Template)을 다운로드 및 실행한다.

SectorC14 그룹의 활동은 우크라이나에서 발견되었다. 해당 그룹은 포털 사이트(Portal Site)로 위장한 피싱 사이트(Phishing Site) 링크를 포함 한 PDF 파일을 첨부한 메일을 사용했으며, 포털 사이트(Portal Site) 보안 경고 내용으로 공격 대상이 PDF 파일을 실행하도록 유도했다.

현재까지 지속되는 SectorC 해킹 그룹들의 해킹 활동은 인접한 국가를 포함한 전 세계를 대상으로 각 국가들의 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

4) SectorD 그룹 활동 특징

SectorD 그룹들 중 이번 6월 총 2개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorD01, SectorD15 그룹이다.

SectorD01 그룹의 활동은 이스라엘, 오스트레일리아에서 발견되었다. 해당 그룹은 VPN 취약점에 노출된 서버를 대상으로 웹쉘(WebShell)을 사용하였으며, 최종적으로 머니버드 랜섬웨어(Moneybird Ransomware)를 배포했다.

SectorD15 그룹의 활동은 사우디아라비아, 이스라엘, 영국에서 발견되었다. 해당 그룹은 운송 및 물류 관련 웹 사이트를 대상으로 워터링 홀(Watering hole) 공격을 시도했으며, 웹 페이지에 삽입된 자바스크립트(JavaScript) 형식의 악성코드는 사이트 방문자의 운영체제 언어, IP 주소, 화면 해상도 정보 등을 수집했다.

SectorD 해킹 그룹들은 주로 정치적인 경쟁 관계에 있는 국가들을 대상으로 해킹 활동을 수행하였으며, 최근의 SectorD 해킹 그룹들의 해킹 활동 목적은 정부에 반대하는 인물 또는 국가들의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

5) SectorE 그룹 활동 특징

SectorE 그룹들 중 이번 6월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE02, SectorE04, SectorE05 그룹이다.

SectorE01 그룹은 영국, 네팔에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 VPN 소프트웨어로 위장한 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 다운로더(Downloader) 기능의 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

SectorE02 그룹은 미국, 파키스탄에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 채팅 앱, VPN 앱으로 위장한 안드로이드(Android) 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 단말기에서 연락처, 위치 정보 등의 민감한 정보를 탈취하였다.

SectorE04 그룹은 파키스탄, 덴마크에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 급여 인상 목록 문서 및 손상된 시스템(Compromised Systems) 목록으로 위장한 MS 엑셀(Excel) 문서를 배포하여 공격 활동을 하였으며, 최종적으로 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

SectorE05 그룹은 파키스탄에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 개발 프로젝트 평가로 위장한 윈도우 도움말 파일을 배포하여 공격 활동을 하였으며, 최종적으로 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

현재까지 지속되는 SectorE 해킹 그룹들의 해킹 활동 목적은 인접한 파키스탄 정부와 관련된 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다. 그러나 최근에는 중국을 포함한 극동 아시아와 다른 지역으로 확대되고 있는 점으로 미루어, 정치, 외교 및 기술 관련 고급 정보들을 획득하기 위한 활동의 비중도 커지고 있는 것으로 분석된다.

6) SectorF 그룹 활동 특징

SectorF 그룹들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorF01 그룹이다.

SectorF01 그룹은 베트남, 체코에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 금융 부문을 대상으로 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 시스템 정보 탈취, 파일 다운로드 및 업로드, 프로세스 인젝션(Process Injection) 등의 악성 행위를 수행하였다.

현재까지 SectorF 해킹 그룹은 이들을 지원하는 정부와 인접한 국가들의 정치, 외교 및 군사 활동과 같은 고급 정보를 수집하기 위한 목적과, 자국의 경제 발전을 위한 첨단 기술 관련 고급 정보 탈취를 위한 목적을 갖는 것으로 분석된다.

7) SectorH 그룹 활동 특징

SectorH 그룹들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorH03 그룹이다.

SectorH03 그룹은 파키스탄, 인도, 중국, 홍콩에서 이들의 활동이 발견되었다. 해당 그룹은 국방 제품 수출 문서 및 보안 조치 문서로 위장한 문서를 배포하여 공격 활동을 하였으며, 최종적으로 크림슨RAT(CrimsonRAT) 악성코드를 설치하여 정보 탈취 행위를 하였다.

SectorH 해킹 그룹의 해킹 활동은 사이버 범죄 목적의 해킹과 정부 지원 목적의 해킹 활동을 병행한다. 특히, 인접한 인도와 여러 가지 외교적 마찰이 계속되고 있어, 목적에 따라 인도 정부 기관의 군사 및 정치 관련 고급 정보들을 탈취하기 위한 활동들을 향후에도 지속적으로 수행할 것으로 분석된다.

8) SectorS 그룹 활동 특징

SectorS 그룹들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorS01 그룹이다.

SectorS01 그룹은 캐나다, 콜롬비아, 브라질, 한국, 프랑스, 홍콩, 스페인에서 이들의 활동이 발견되었다. 해당 그룹은 엠바고(Embargo) 요청으로 위장한 어도비(Adobe) PDF 문서를 배포하여 공격 활동을 하였으며, 정보 탈취 행위를 하였다.

현재까지 지속되는 SectorS 해킹 그룹의 해킹 활동 목적은 인접한 남미 지역의 국가들에서 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다.

9) Cyber Crime 그룹 활동 특징

온라인 가상 공간에서 활동하는 사이버 범죄 그룹은 이번 6월에는 총 7개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ04, SectorJ09, SectorJ20, SectorJ27, SectorJ39, SectorJ110, SectorJ118 그룹이다.

이들은 다른 정부 지원 해킹 그룹들과 다르게 현실 세계에서 금전적인 이윤을 확보할 수 있는 재화적 가치가 있는 온라인 정보들을 탈취하거나, 직접적으로 특정 기업 및 조직들을 해킹 한 후 내부 네트워크에 랜섬웨어(Ransomware)를 유포하거나, 중요 산업 기밀을 탈취한 후 이를 빌미로 금전적 대가를 요구하는 협박 활동 등을 수행한다.

SectorJ04 그룹의 활동은 미국, 영국, 인도, 이탈리아, 캐나다, 아일랜드, 싱가포르에서 발견되었다. 해당 그룹은 MOVEit Transfer 취약점(CVE-2023-35708, CVE-2023-34362)에 노출된 시스템을 대상으로 클롭 랜섬웨어(Cl0p Ransomware)를 배포했다.

SectorJ09 그룹은 웹 사이트에 난독화 된 스키밍(Skimming) 스크립트를 삽입하여, 결제 페이지에서 사용자명, 주소, 메일, 전화번호와 신용카드 지불 정보 등을 수집하는 기존의 해킹 방식을 유지하고 있다.

SectorJ20 그룹의 활동은 영국에서 발견되었다. 해당 그룹은 여권 사진으로 위장한 윈도우 바로가기(LNK) 파일 형식의 악성코드를 사용했으며, 실행 시 난독화 된 배치(Batch) 스크립트 형식의 명령줄을 통해 추가 악성코드를 다운로드 및 실행한다.

SectorJ27그룹의 활동은 러시아, 중국, 오스트리아, 폴란드, 싱가포르, 몰도바, 독일, 아르헨티나, 불가리아, 터키, 미국, 남아프리카, 이탈리아, 벨라루스, 대만, 말레이시아, 알제리, 캐나다, 그루지야, 우크라이나, 스위스에서 발견되었다. 해당 그룹은 국제 운송 기업을 사칭한 피싱 메일에 MS 워드(Word) 악성코드를 첨부했으며, 최종적으로 원격 제어 기능을 가진 악성코드를 시스템에 설치하여 시스템 정보 수집 및 명령 및 제어를 시도했다.

SectorJ39 그룹의 활동은 러시아, 체코, 미국, 우크라이나, 오스트레일리아에서 발견되었다. 해당 그룹은 검색 결과 최상단에 광고를 게시하는 구글애즈(Google Ads)를 악용하여 피싱 사이트(Phishing Site) 접속을 유도했으며, 최종적으로 시스템 권한 탈취 및 명령 제어를 할 수 있는 악성코드를 사용했다.

SectorJ110 그룹의 활동은 우크라이나, 스페인에서 발견되었다. 해당 그룹은 내부에 청구서로 위장한 자바스크립트(JavaScript) 파일 형식의 악성코드가 존재하는 압축파일을 첨부하여 피싱 메일(Phishing Mail)을 배포했으며, 최종적으로 추가 악성코드를 다운로드 및 실행할 수 있는 기능을 가진 악성코드를 사용했다.

SectorJ118 그룹의 활동은 미국, 캐나다, 리투아니아에서 발견되었다. 해당 그룹은 불법 콘텐츠(Illegal Content)를 호스팅하는 웹 사이트를 악성코드 배포에 악용했으며, 최종적으로 사용한 크롬 브라우저 확장프로그램(Chrome Browser Extension) 악성코드는 브라우저 검색 정보 같은 민감한 정보를 수집하고, 임의의 광고를 브라우저에 삽입하는 기능을 가지고 있다.

한국 내 대북분야 종사자 겨냥 BitB 공격 동향 분석

문종현 이사(센터장), 지니언스 시큐리티 센터(GSC), chmun@genians.com

주요 요약(Executive Summary)

- 미국 내 국제비정부단체 링크 (LiNK)의 탈북민 활동 지원금 프로그램 사칭 공격
- 단체에서 운영하는 페이스북 내용을 그대로 모방해 정교한 피싱 사이트 개설
- ‘Browser In The Browser(BitB)’ 공격 기술을 적용해 대북활동 전문가 현혹
- 평소 쉽게 접할 수 있는 ‘Single Sign-On (SSO)’ 서비스로 위장해 접근
- 거점 서버의 흐름을 추적한 결과, 북한 배후 해킹 그룹 APT37 인프라 연결 발견

1. 개요(Overview)

1) 국제 북한인권단체를 사칭한 위협 식별 (Threat Hunting)

지난 7월 24일 지니언스 시큐리티 센터(이하 GSC)는 북한 연계 해킹그룹의 소행으로 분류된 새로운 공격 징후를 포착했다. GSC는 이번 위협이 국내외 대북 전문가의 일상생활 감시와 개인 정보 탈취에 목적을 둔 사이버 첩보전 일환으로 보고 있다.

공격자는 국제 비정부단체인 ‘링크[LiNK : Liberty in North Korea]’에서 실제로 진행 중인 ‘체인지메이커 활동 지원금 프로그램' 모집 내용을 교묘히 사칭했다. 해당 단체는 북한 인권 개선과 탈북 지원 활동 등으로 알려져 있다.

해당 프로그램은 북한 출신 활동가를 대상으로 하고 있으며, 실제 지원 기한은 7월 26일로 공격이 확인된 24일 기준 약 2일의 여유가 있었다. 총 금액은 600만원으로 매달 50만원씩 12개월간 활동 지원금을 제공하게 된다. 나름 촉박한 신청 기한을 감안한다면 공격 대상자를 현혹하는데 충분한 요소로 볼 수 있다.

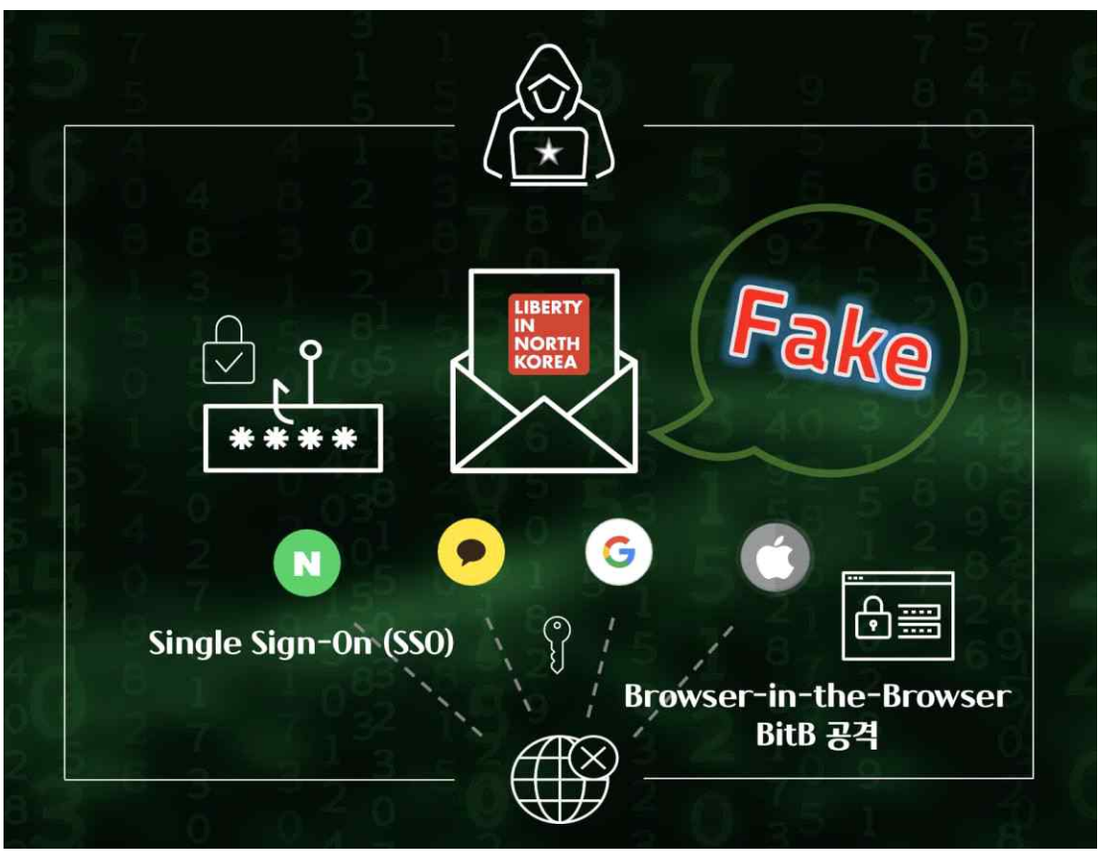
안내 포스터에 담긴 구체적 모집 대상을 살펴보면, ▶인권 옹호 및 인식 개선 활동 ▶북한 사람 중심의 콘텐츠 제작 및 배포 ▶탈북인 정착 지원 및 역량 강화 ▶기타 북한 사람들을 위한 활동 등 주로 북한 출신 활동 내용이 담겨 있다. 따라서 해당 위협은 탈북민이나 유관 단체가 주요 타깃에 해당될 수 있다.

2) 피싱 공격 흐름 (Phishing Attack Flow)

본격적인 공격은 이메일 내 상세 내용을 보려면 별도의 홈페이지 주소를 참고하라는 식으로 계정 해킹을 유인하는데, 실제 해당 프로그램에서 배포한 내용을 그대로 모방했다. 만약, 해당 내용에 속아 공격자가 직접 개설한 가짜 사이트로 연결되면, 피싱 공격이 진행된다.

마치 탈북민의 북한인권 활동 지원 프로그램처럼 조작된 피싱 이메일로 공격이 수행된다. 이메일 본문에 삽입된 가짜 홈페이지 주소에 접근할 경우 계정 탈취 목적의 피싱 사이트가 나타난다. 이때 입력된 이메일 주소와 비밀번호가 공격자에게 유출되는 과정을 거친다.

[그림 1] 피싱 공격 간략 흐름도



3) 공격 전술 및 기술, 절차 (TTPs) & BitB 공격

현존하는 미국의 북한인권 단체와 공식적으로 알려진 탈북민 활동지원 프로그램을 사칭해 시기적절한 맞춤형 전술 공격을 사용했다. 공격자는 해당 단체가 운영하는 페이스북 내용을 모방해 사용했으며, 북한 출신 활동가를 겨냥해 이메일 피싱 공격에 활용했다.

[그림 2] 링크(LiNK) 단체 공식 페이스북 안내문 화면

공격자는 다수의 탈북민 및 대북단체를 상대로 해당 공격을 수행했다. 특히, 일반적으로 많이 쓰이는 SSO(Single Sign-On) 단일 인증 방식을 공격에 접목했다.[1)]

공격 거점으로 사용할 피싱용 도메인과 웹 서버를 직접 구축했고, 'Browser In The Browser(BitB)' 공격 기술을 사용했다.[2)]

합법적인 웹 브라우저와 주소로 보이게 위장하는 것이 피싱 공격 성공의 가장 중요한 요소인 점을 감안한다면, 허위로 조작된 피싱 사이트가 공식 URL 주소처럼 보이게 만드는 것은 핵심적인 공격 절차 중 하나이다.

BitB 공격 기술은 웹 브라우저 내부에 인증 용도로 조작된 또 다른 팝업 창을 추가로 보여주는 피싱 수법이다. 이때 보인 웹 브라우저 화면과 URL 내용은 신뢰 가능한 공식 주소처럼 보이게 디자인이 가능하다. 따라서 겉으로 보이는 URL 주소만 믿고 비밀번호를 입력할 경우 해킹 피해를 입게 된다.

GSC는 본 피싱 공격이 BitB 공격 기술을 절묘하게 사용한 점에 주목했다. 이번 보고서 사례처럼 외관상 보여지는 URL 주소의 진위여부를 판단하는데 보다 세심한 주의와 관심이 필요한 이유이다. 육안상 인지된 주소만을 믿고 접근해 함부로 개인정보를 입력할 경우 예기치 못한 위협에 노출될 가능성이 높다.

BitB 공격을 감지하는 방법 중 하나는 팝업 로그인 창을 웹 브라우저 가장자리로 드래그(이동)하는 것이다. 팝업 창이 브라우저 화면 밖으로 벗어날 수 없다면 그것은 독립된 실제 창이 아니다.

더불어 본인이 사용하는 웹 브라우저의 유저 인터페이스(UI)와 일관된 디자인과 화면 모드를 유지하고 있느냐 비교하는 것이다. 웹 브라우저의 버튼이나 아이콘 등 구성 디자인 요소에 차이점이 없는지 면밀히 비교해 보는 것이다.

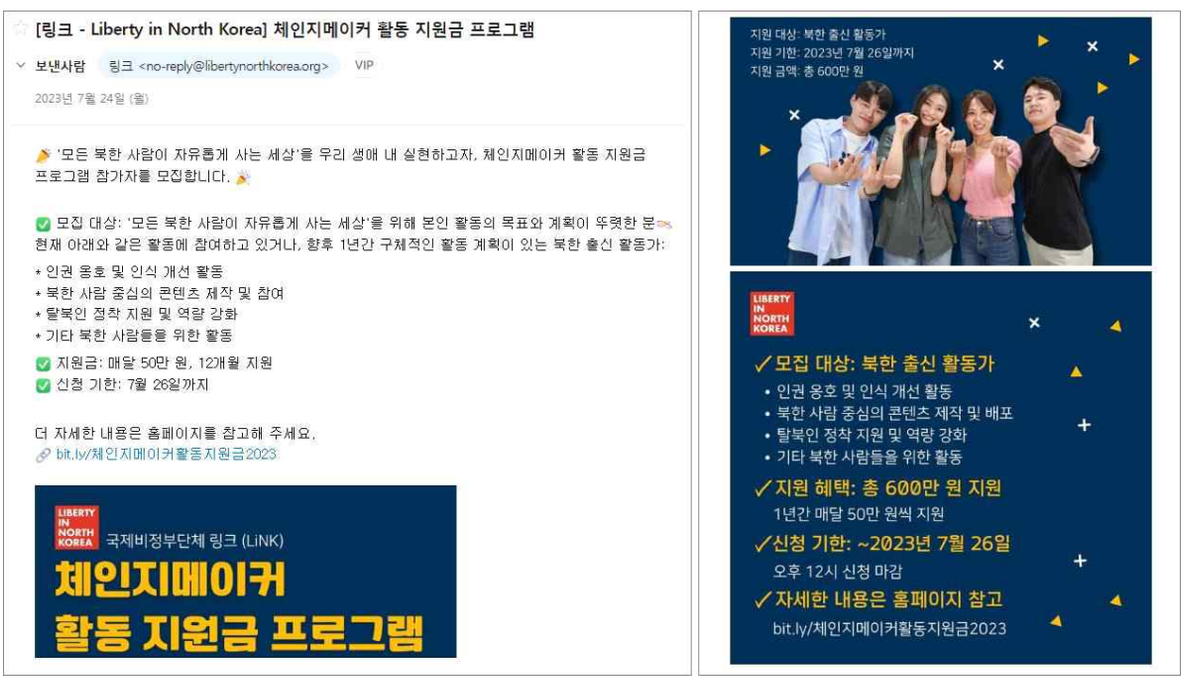
1) https://aws.amazon.com/ko/what-is/sso/
2) https://mrd0x.com/browser-in-the-browser-phishing-attack/

2. 공격 시나리오 (Attack Scenario)

1) 초기 접근 단계-피싱 (Initial Access-Phishing)

실제 공격에 사용된 이메일은 정교하게 제작된 것을 알 수 있다. 본문 내용 하단에 이미지로 포스터가 세로로 길게 포함된 형태이다. 이미지 바로 상단 영역에 피싱 공격용 링크가 'bit.ly' 단축 URL 주소처럼 삽입되어 있다.

[그림 3] 실제 공격에 사용된 이메일 화면



먼저 공격 발신지 주소와 피싱 거점이 동일하게 사용되었다. 이메일 보낸 이 주소는 마치 응답 없는 발송 전용 주소처럼 보이도록 'no-reply@libertynorthkorea[.]org' 주소가 사용됐는데, 공격에 따라 'info' 아이디가 사용되기도 한다.

피싱 사이트로 연결된 도메인 역시 'libertynorthkorea[.]org' 주소가 사용됐는데, 실제 정상 사이트 주소와 비교해 보면 조금 다른 것을 알 수 있다. 정상 사이트의 경우 도메인 중간에 [in] 단어가 포함된 'libertyinnorthkorea[.]org' 주소이다. 따라서 얼핏 보기에 가짜 사이트에 현혹된 가능성이 매우 높은 편에 속한다.

2) 피싱 메일 분석 (Phishing Email Analysis)

공격자는 'titan[.]email' 〈(구)flockmail[.]com〉 이메일 플랫폼 서비스를 악용해 피싱 공격을 수행한다. 이 서비스를 활용한 공격은 북한 연계 해킹 조직이 종종 사용하고 있다.[3)]

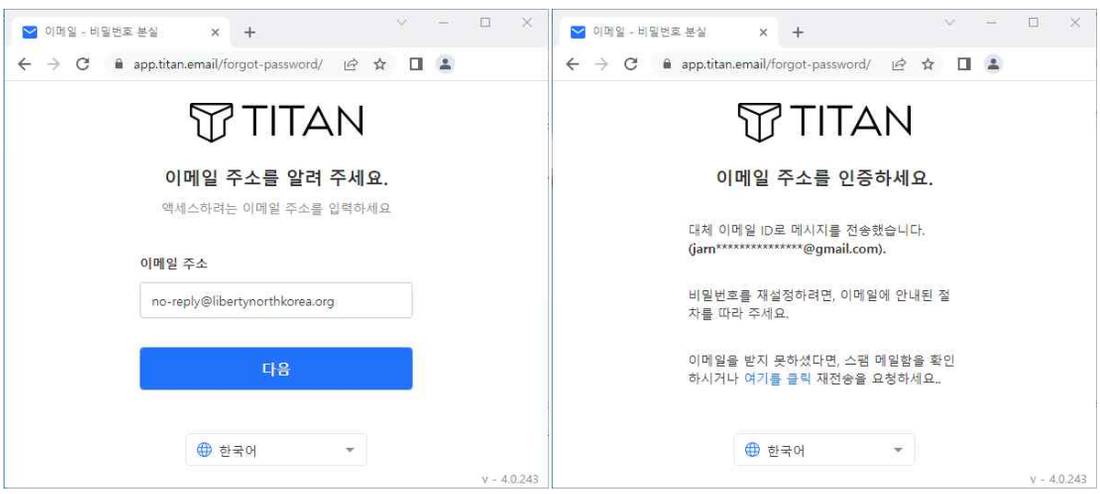
3) https://titan.email/about/

참고로 타이탄 이메일 서비스는 인도 출생 '바빈 투라키아(Bhavin Turakhia)'가 설립한 회사로, 위키디피아에 따르면, 인도에서 순자산이 많은 사람으로 선정된 바 있다. 이 인물은 인도의 온라인 교육 및 경쟁 프로그래밍 플랫폼인 코드쉐프(CodeChef) 설립에 참여한 것으로 알려져 있다.[4)]

흥미롭게도 코드쉐프는 국제 소프트웨어 프로그래밍 경진대회로 북한 김일성 종합대, 김책공대 학생들이 지난 2013년부터 경연에 참가해 수차례 우승을 차지한 것으로 알려져 있다.[5)]

현재 해킹 공격에 쓰이는 해외 이메일 플랫폼 서비스와 북한 학생들이 수년간 참여한 국제 프로그래밍 경연 대회의 연관성을 단순 우연으로 볼지는 앞으로 보다 심도 있게 관찰할 필요가 있다.[6)]

[그림 4] 타이탄 이메일에 등록된 대체 메일 주소 화면



앞서 공격에 사용된 발신지 'no-reply@libertynorthkorea.org' 메일 주소를 타이탄 서비스로 조회해 보면, 'jarn**********@gmail.com' 지메일을 대체 주소로 사용한 것을 알 수 있다. 자세히 보면, 영문 알파벳 R과 N을 소문자로 연이어 사용한 전형적 패턴을 볼 수 있는데, 보통 m 문자처럼 보이기 위한 수법이다.

이메일 내부 하단 위치에 수신 여부 등을 체크하기 위해 웹 비콘(Web Beacon) 이미지 기능이 숨겨져 있는데, 이때 사용된 도메인 주소는 'help.naver.com[.]de' 이다.

4) https://en.wikipedia.org/wiki/Bhavin_Turakhia
5) http://monthly.chosun.com/client/mdaily/daily_view.asp?idx=2122&Newsnumb=2017112122
6) https://www.hankyung.com/opinion/article/2023070719441

[그림 5] 이메일 내부에 숨겨져 있는 비콘 코드 화면

```
=3D"_blank" style=3D"color: rgb(0, 123, 217); cursor:
pointer; text-decorat=
ion: none; border: 0px; outline: none; list-style: none;
margin: 0px; text-=
align: inherit; padding: 0px; box-sizing: border-box;
touch-action: manipul=
ation; background-color: rgba(0, 0, 0, 0); display:
inline; font-family: in=
herit;">bit.
ly/=EC=B2=B4=EC=9D=B8=EC=A7=80=EB=A9=94=EC=9D=B4=EC=BB=A4=
=ED=99=9C=EB=8F=99=EC=A7=80=EC=9B=90=EA=B8=882023</a></spa
n></div><div styl=
e=3D"text-align: left;"><br></div></div></div>

</div>
<img src=3D"https://libertynorthkorea.
org/assets/media/           /35837970=
3_316934690663613_4979253201212185035_n.jpg"
width=3D"450px" height=3D"450p=
x">
<img src=3D"https://libertynorthkorea.
org/assets/media/           /35806292=
4_316934693996946_7643035514259184264_n.jpg"
width=3D"450px" height=3D"450p=
x">
</div><img src=3D'https://help.naver.com.de
/asset/media/   /background.jpg?=
```

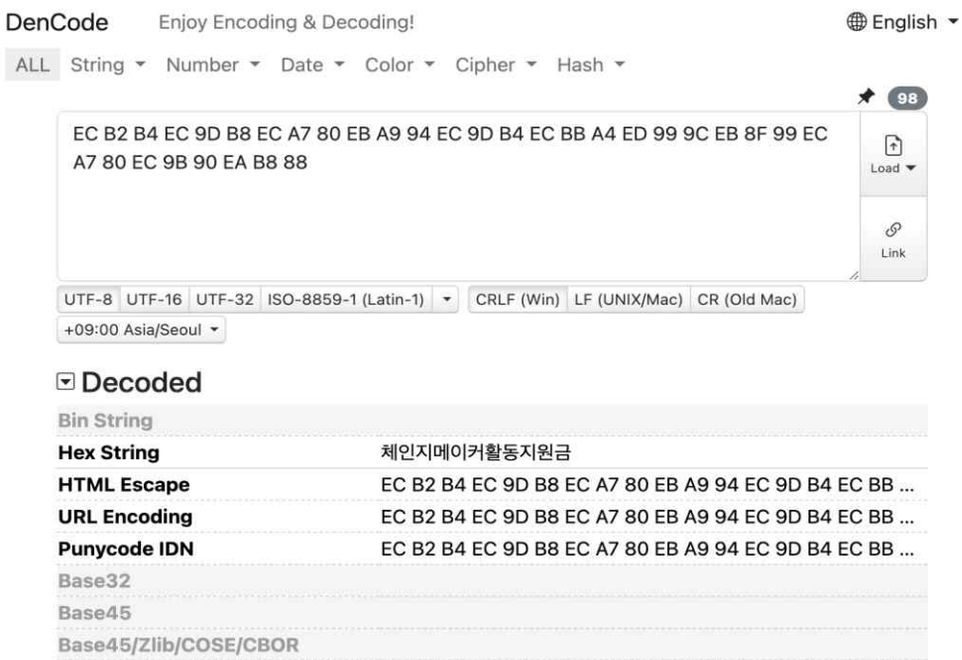
웹 비콘 상단에 위치한 피싱 링크(bit.ly/체인지메이커활동지원금2023) 주소는 한글 표기가 포함되어 있고, UTF-8 데이터가 포함되어 있다. 해당 코드는 DenCode 사이트에서 한글로 쉽게 변환이 가능하다.[7)]

[표 1] 피싱 링크로 사용된 데이터 화면

EC B2 B4 EC 9D B8 EC A7 80 EB A9 94 EC 9D B4 EC BB A4 ED 99 9C EB 8F 99 EC A7 80 EC 9B 90 EA B8 88

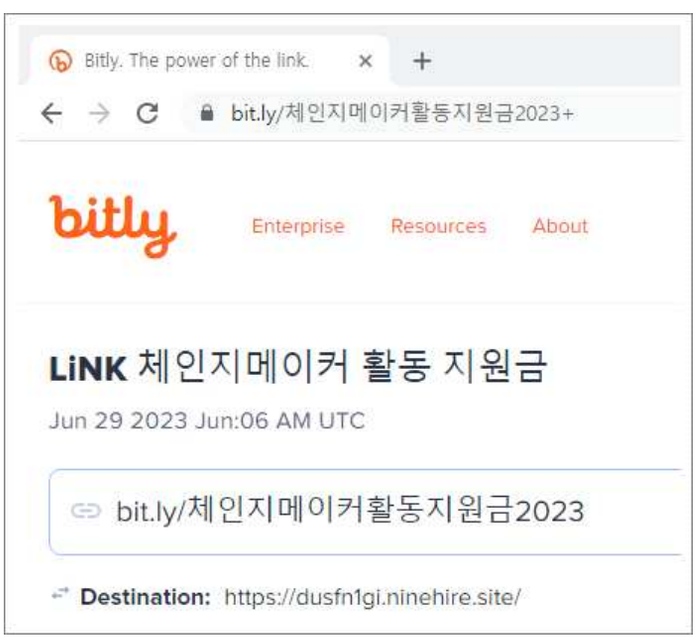
7) https://dencode.com/

[그림 6] DenCode 서비스로 변환된 한글 문자열 화면



외관상 보여지는 Bitly 단축 URL 서비스의 최종 연결 주소는 6월 29일에 등록됐으며, (dusfn1gi.ninehire[.]site) 정상 LiNK 체인지메이커 활동 지원금 서비스로 연결된 것을 확인할 수 있다.

[그림 7] 실제 정상 단축 URL 주소 화면



하지만 단축 URL 내부 링크는 피싱 서버 'libertynorthkorea[.]org' 주소로 연결돼 있으며, 토큰 인자 값이 없을 경우에는 공식 사이트로 전환시켜 분석을 회피한다.

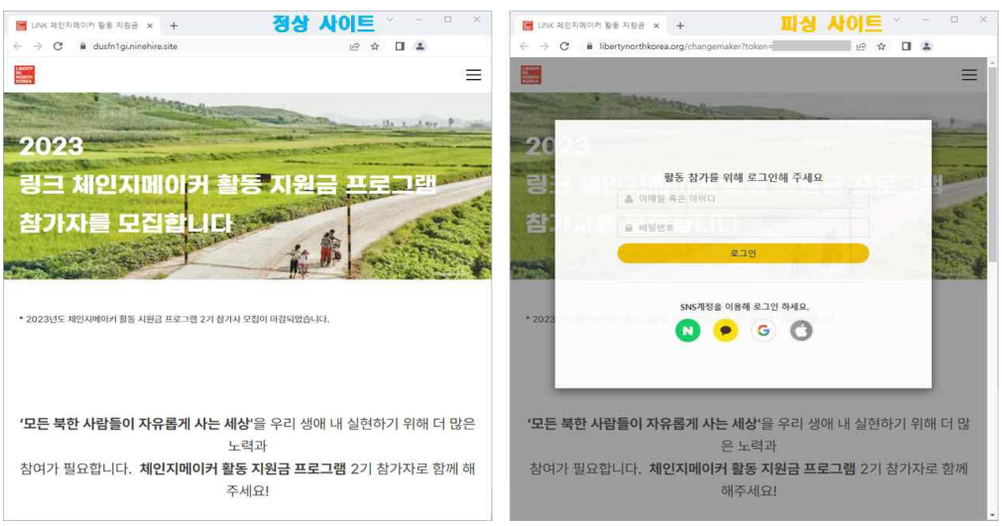
[그림 8] 해킹 이메일에 쓰인 단축 URL 주소 화면

3. 피싱 위협 분석 (Phishing Threat Analysis)

1) 정교한 유사 웹 사이트 구축

피해 대상자가 'libertynorthkorea[.]org' 주소를 클릭해 접근하면, 정교하게 디자인된 가짜 웹 사이트가 나타난다. 정상 사이트와 피싱용으로 제작된 가짜 사이트를 비교해 보면 로그인 창 팝업 여부가 다른 점을 볼 수 있다.

[그림 9] 정상 사이트(좌)와 피싱 사이트(우) 비교 화면



피싱 사이트는 원래 정상 웹 사이트(dusfn1gi.ninehire[.]site)의 내용을 그대로 보여주도록 아이프레임을 구성했다. 여기서 눈에 띄는 점은 아이프레임 아이디 값이 조선뉴스(chosunnews)라는 점이며, 웹 페이지 종속 스타일 시트(Cascading Style Sheet) 파일도 'chosun.css' 파일명을 사용했다. GSC는 해당 피싱 사이트를 조사하는 과정 중에 공격자가 조선일보(chosun[.]com) 웹 사이트의 폰트 설정 및 'style.css' 값을 일부 활용한 점을 확인했다.

[표 2] 피싱 사이트의 아이프레임 코드 화면

```
〈iframe id="chosunnews" src="https://dusfn1gi.ninehire.site/"
style="width:100%;height:100%;border-width:0px;"
scrolling="no"〉〈/iframe〉
```

2) BitB 피싱 공격 기술

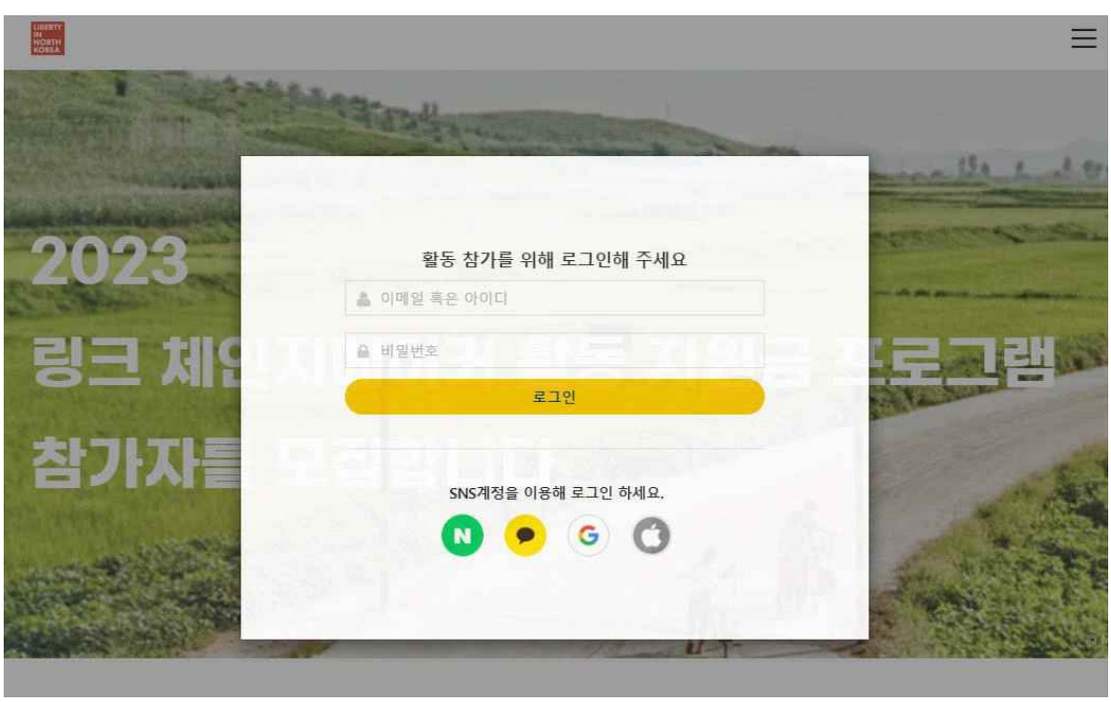
피싱 공격용 웹 사이트는 공식 Liberty in North Korea (libertyinnorthkorea[.]org) 도메인 주소와 유사하게 만든 점이 특징이다.

[표 3] 공식 사이트와 피싱 사이트 도메인 비교

정상 도메인	libertyinnorthkorea[.]org	dusfn1gi.ninehire[.]site
피싱 도메인	libertynorthkorea[.]org	-

조작된 사이트로 연결되면 '활동 참가를 위해 로그인해 주세요' 타이틀을 가진 팝업 창이 나타난다. 자체 이메일 로그인 유도 화면과 'SNS계정을 이용해 로그인 하세요'라는 내용의 SSO(Single Sign-On) 단일 인증 방식 아이콘을 보여준다.

[그림 10] 피싱 사이트 접근 시 보여지는 팝업 창 화면



이메일 혹은 아이디와 비밀번호 수동 입력을 통한 직접적 로그인 계정 탈취 방식을 사용할 뿐만 아니라, ▶네이버 ▶카카오 ▶구글 ▶애플 등의 계정이 선택적으로 유출될 수 있는 방식이다.

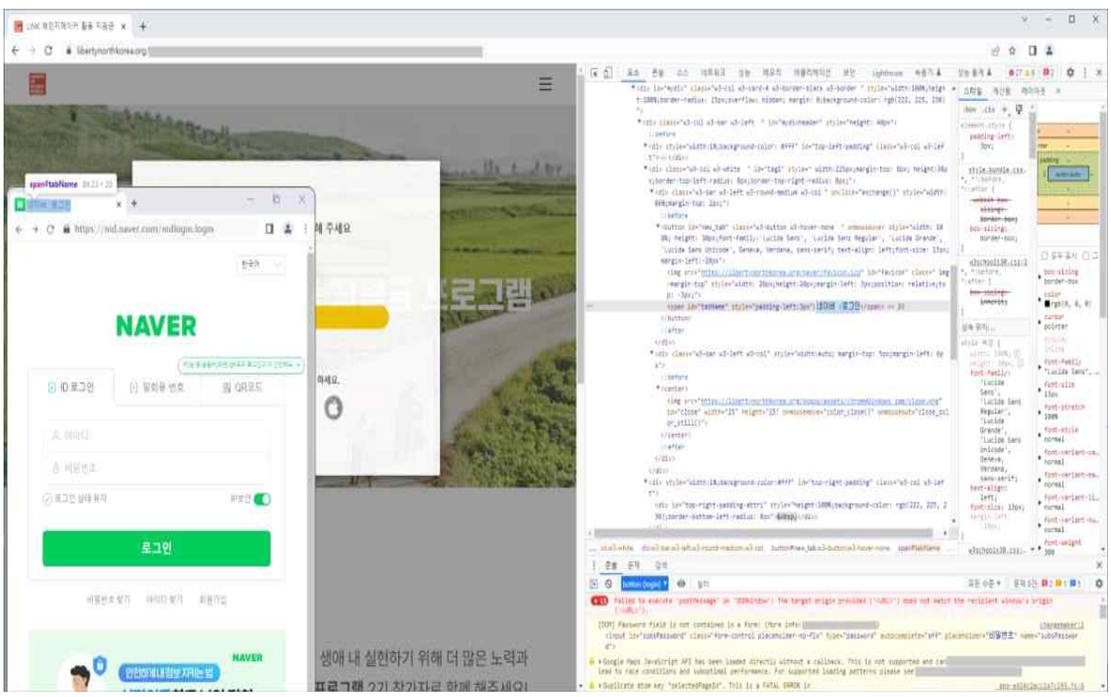
SSO 통합적 단일 인증 방식은 번거로운 별도의 가입절차가 없어 편의상 많이 쓰이고 있다. 평소 접해 보지 못한 생소한 웹 사이트에 신규로 가입하거나 로그인하는 것은 보안상 매우 조심스러운 부분이다. 일반적으로 악성 의심 사이트를 구별하는데 있어, 절차상 가장 우선시되는 점은 웹 브라우저상 접속 주소일 것이다. 주소창에 보이는

인터넷 URL 경로가 내가 기존에 잘 알고 있던 도메인이라면 충분히 신뢰하고 로그인을 진행할 것이다.

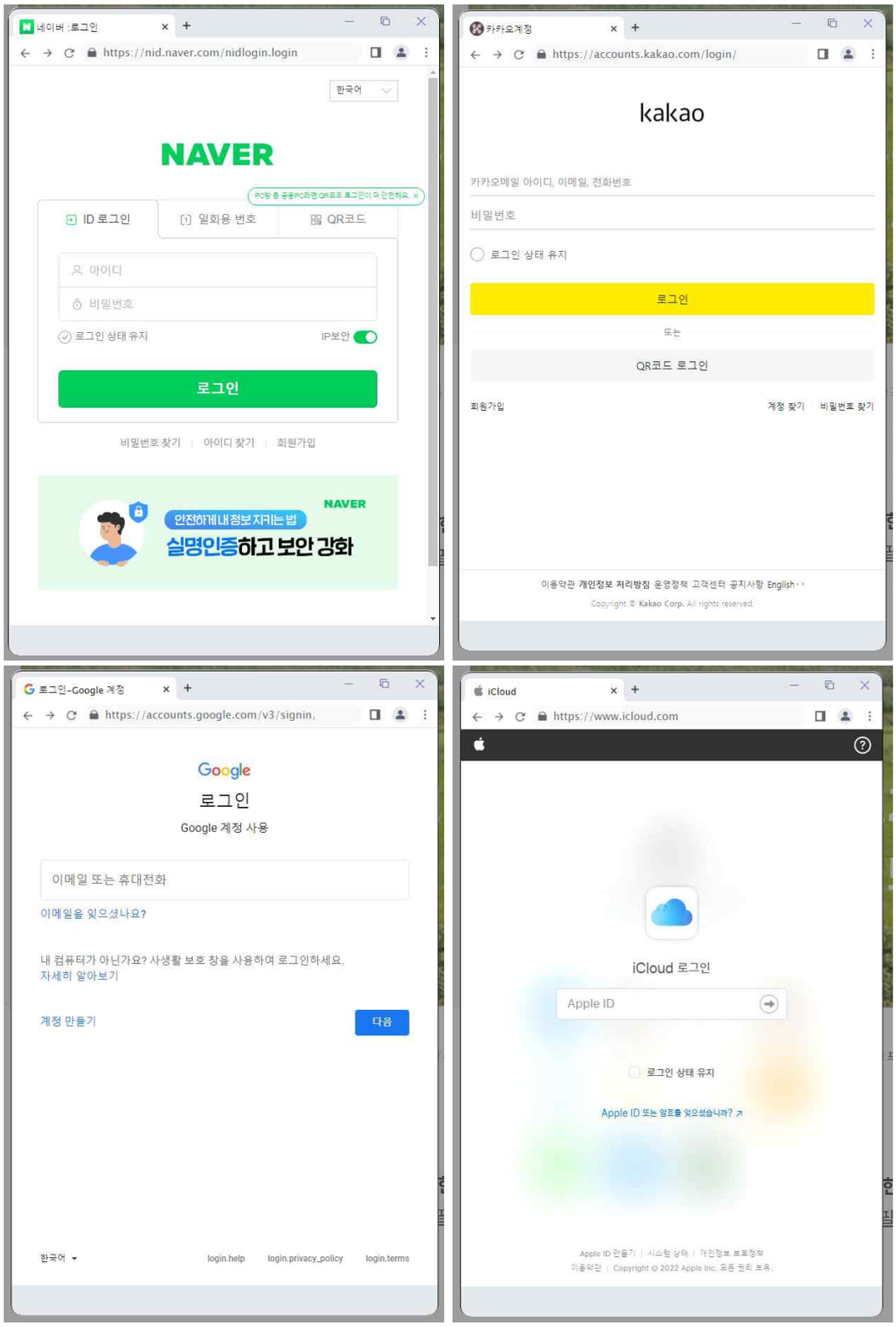
더구나 앞서 설명한 'Browser In The Browser(BitB)' 공격 기술을 사전에 숙지하지 못했다면, 이러한 공격에 쉽게 노출될 수 있다. 쉽게 말해, 웹 브라우저 내부에 또 다른 가짜 웹 브라우저 화면을 디자인해 띄우는 절묘한 속임수 기법이다. 공식 URL 주소가 포함된 팝업 창을 띄우는 것이기 때문에 주소창에 입력된 도메인 자체를 공격자가 얼마든지 임의로 설정할 수 있다.

공격자는 팝업 창의 스타일과 클래스, 아이콘, 이미지 연결 등을 디자인해 마치 포털 사의 공식 로그인 서비스처럼 화면을 만들었다. 더불어 국내외 기업의 계정 정보 탈취가 가능하도록 다양한 로그인 팝업 창을 제작해 두었다.

[그림 11] 가짜 로그인 팝업 창과 내부 코드 화면



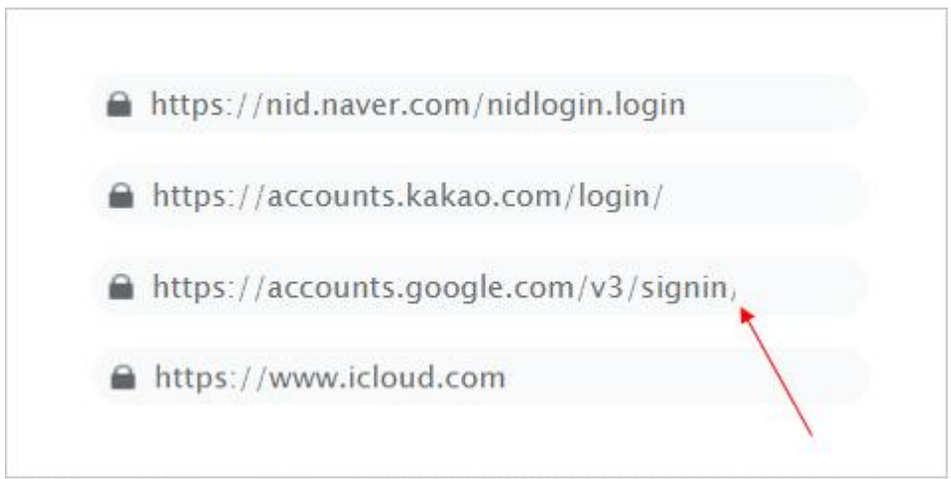
[표 4] BitB 기법의 피싱용 팝업 창 화면 비교



상기 서비스별 가짜 팝업 창을 살펴보면, 나름 실제 서비스처럼 보이도록 정교하게 모방했다. BitB 공격의 가장 치명적 위협 요소는 바로 정상 URL 주소가 보인다는 점이다.

각 팝업 로그인 창에 삽입된 URL 주소를 하나씩 추출해 비교해 보면, 실제 공식 회사의 도메인 사이트가 포함된 것을 알 수 있다. 단순히 영어 알파벳을 유사하게 만든 전형적인 웹 피싱 기법과 다르게 정상 인터넷 주소가 보이도록 조작한 것이 핵심이다.

[그림 12] BitB 피싱 로그인 창 화면의 디자인된 URL 주소 화면

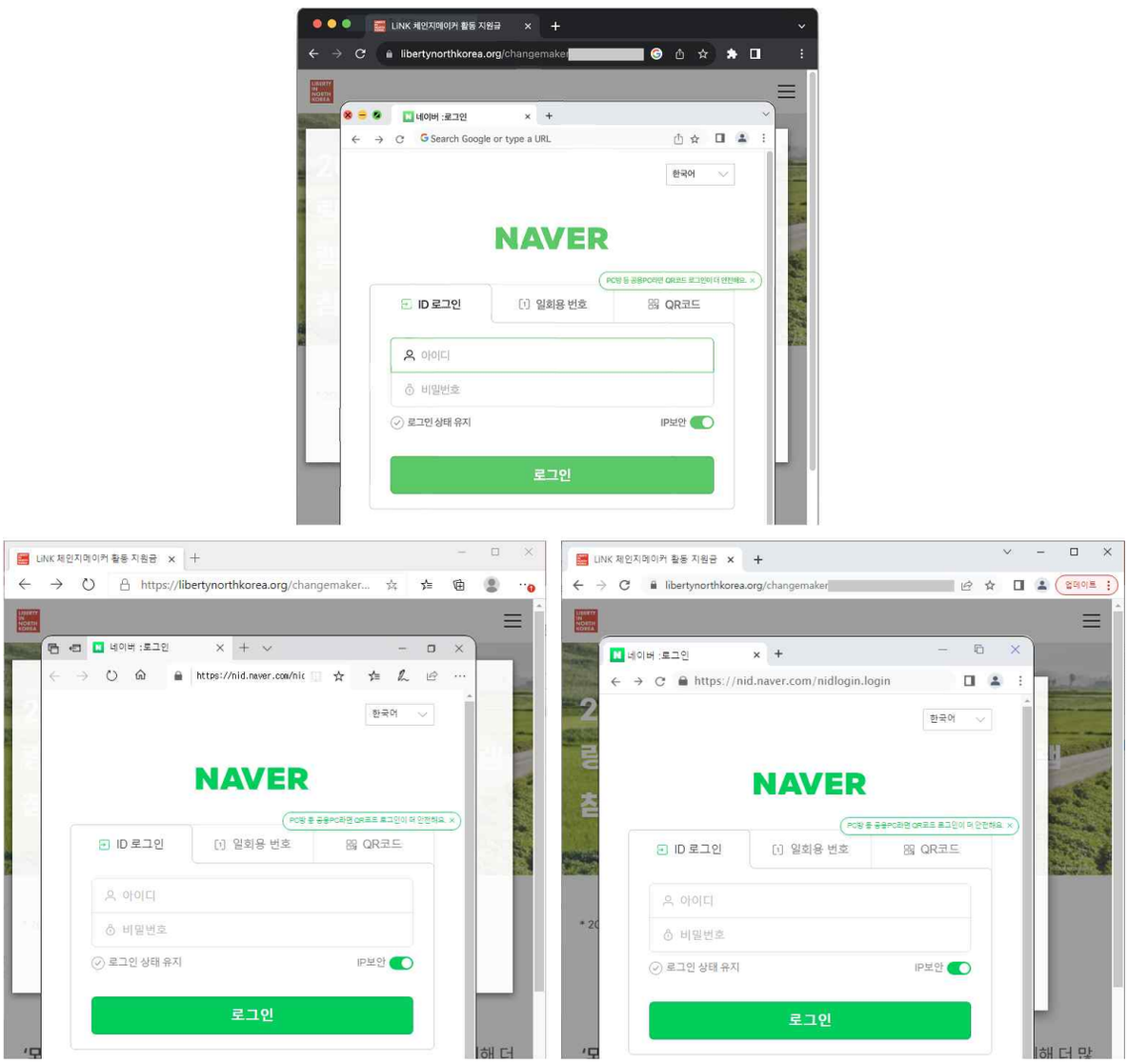


물론, 여기에도 허점은 존재한다. 구글 피싱 사이트의 경우 주소 가장 끝단의 슬래시(/) 부분 영역 일부가 잘려 보이는 현상이 목격된다. 그리고 BitB 주소 창 영역의 페이지 공유 및 탭 북마크 추가 아이콘이 보이지 않을 수 있다.

아울러 화면을 다크 모드로 설정해 사용하는 등 이용자 환경의 개별 조건에 따라 사전에 의심해 볼 만한 여지가 충분히 존재하거나 발견해 낼 수도 있다. 이외에 창 테두리나 모서리 화면이 사용 중인 웹 브라우저와 상이하거나 어눌하게 표시된 점도 확인할 수 있다.

이처럼 얼핏 보기에 실제 사이트로 혼동할 수 있다는 점에서 각별한 주의가 필요한 부분이다. 그리고 공격자는 macOS Chrome, MS Edge, Google Chrome 등 웹 브라우저 종류에 따라 나름 맞춤형 디자인을 적용했다.

[그림 13] OS 및 웹 브라우저별 비교 화면



BitB 공격 여부를 가장 쉽고 정확하게 확인하는 방법은 팝업 창이 현재 사용 중인 웹 브라우저 영역 밖으로 이동이 가능한지를 보는 것이다. BitB 피싱의 경우 팝업 창 자체가 단순히 별도의 웹 브라우저처럼 디자인으로 위장된 것이지 완전히 독립된 상태가 아니다. 따라서 기존 웹 브라우저 내에서만 이동이 가능한 고유한 특성을 활용한 방안이 있다.

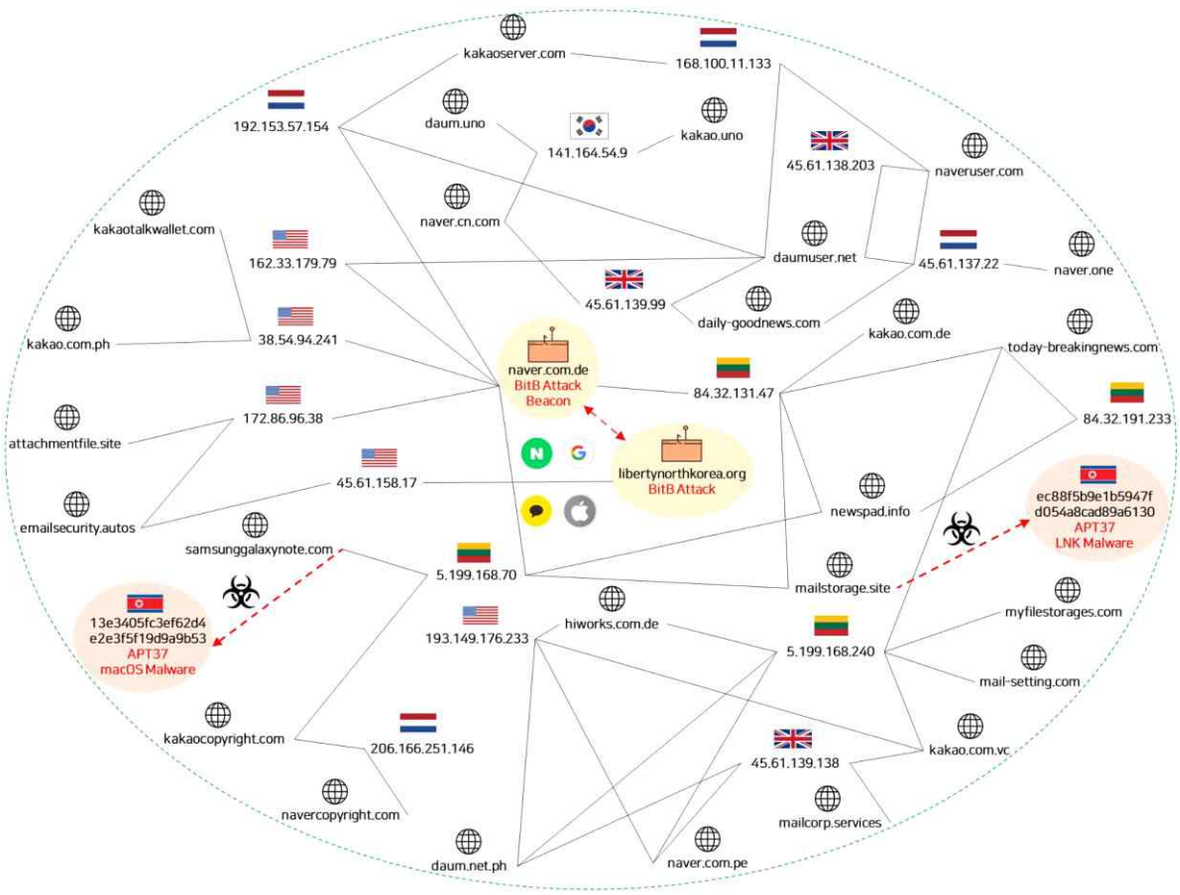
4. 위협 인프라 유사도 (Similarity)

1) BitB 피싱과 APT37 공격 거점의 연결 고리

GSC는 BitB 공격에 활용된 위협 지표를 조사하는 과정에서 APT37 공격 인프라와 연결된 고리를 찾았다.

이번 BitB 피싱 공격에 활용된 'libertynorthkorea[.]org' 도메인은 분석 시점 당시 미국 아이피 '45.61.158[.]17' 주소로 연결되었으며, 'ru.emailsecurity[.]autos' 도메인도 동일한 아이피가 사용되었다. 서브 도메인 중 'protect.emailsecurity[.]autos' 주소가 존재하며, '172.86.96[.]38' 주소로 연결된다.

[그림 14] BitB 공격 도메인과 APT37 공격 연관성 화면

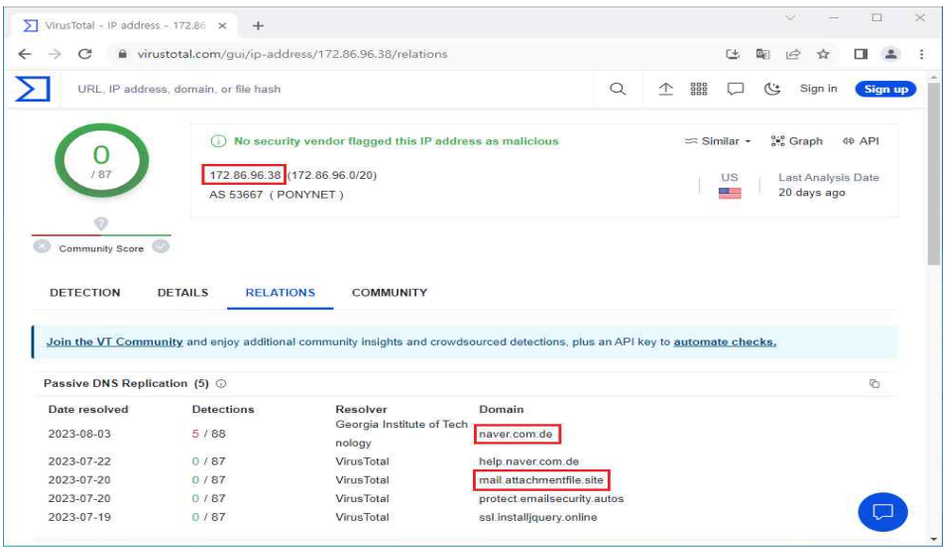


'172.86.96[.]38' 아이피에 연결됐던 Passive DNS 이력을 조회해 보면, 마치 국내 포털사처럼 위장된 'naver.com[.]de' 도메인이 사용된 기록을 확인할 수 있다. 참고로 여기서 언급된 Passive DNS란, 특정 (악성) 도메인이 DNS 쿼리를 통해 IP Lookup된 휘발성 히스토리를 누적해 기록해 둔 것으로, 특정 기간 동안 이뤄지는 네트워크 위협 활동을 조사하는데 의미 있는 위협 인텔리전스 정보로 활용된다.

이렇게 확인된 'naver.com[.]de' 도메인의 경우, 앞서 설명된 해킹메일 본문 내 숨겨진 비콘 도메인과 동일한 것을

볼 수 있다. 단순 우연으로 위협 인프라가 오버랩 된 것이 아니라, 계획적으로 활용됐을 가능성이 높은 이유이다.

[그림 15] 바이러스 토탈 '172.86.96.38' 관계 결과 화면



'naver.com[.]de' 도메인은 '84.32.131[.]47' 리투아니아 소재의 아이피로 할당된 바 있는데, 해당 인프라는 다수의 위협 지표로 사용되었다. 특히, 국내 언론사 웹 사이트처럼 위장한 'newspad[.]info' 도메인의 서브 주소가 대표이다.

'5.199.168[.]70' 아이피 주소의 경우 ▶samsunggalaxynote[.]com 스마트폰 사칭 주소를 포함해 ▶attachment.mailstorage[.]site ▶today-breakingnews[.]com 도메인과도 연결된 바 있고, 기존 APT37 그룹이 사용한 곳이다.

[표 5] 언론사 도메인으로 위장한 침해지표 비교 화면

언론사명	(Sub) Domain 주소		IP 주소 (국가코드)
뉴데일리	공식	newdaily.co[.]kr	[생략]
	피싱	newdaily.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
조선일보	공식	chosun[.]com	[생략]
	피싱	chosun.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
국민일보	공식	kmib.co[.]kr	[생략]
	피싱	kmib.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
연합뉴스	공식	yonhapnews.co[.]kr	[생략]
	피싱	yonhap.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)

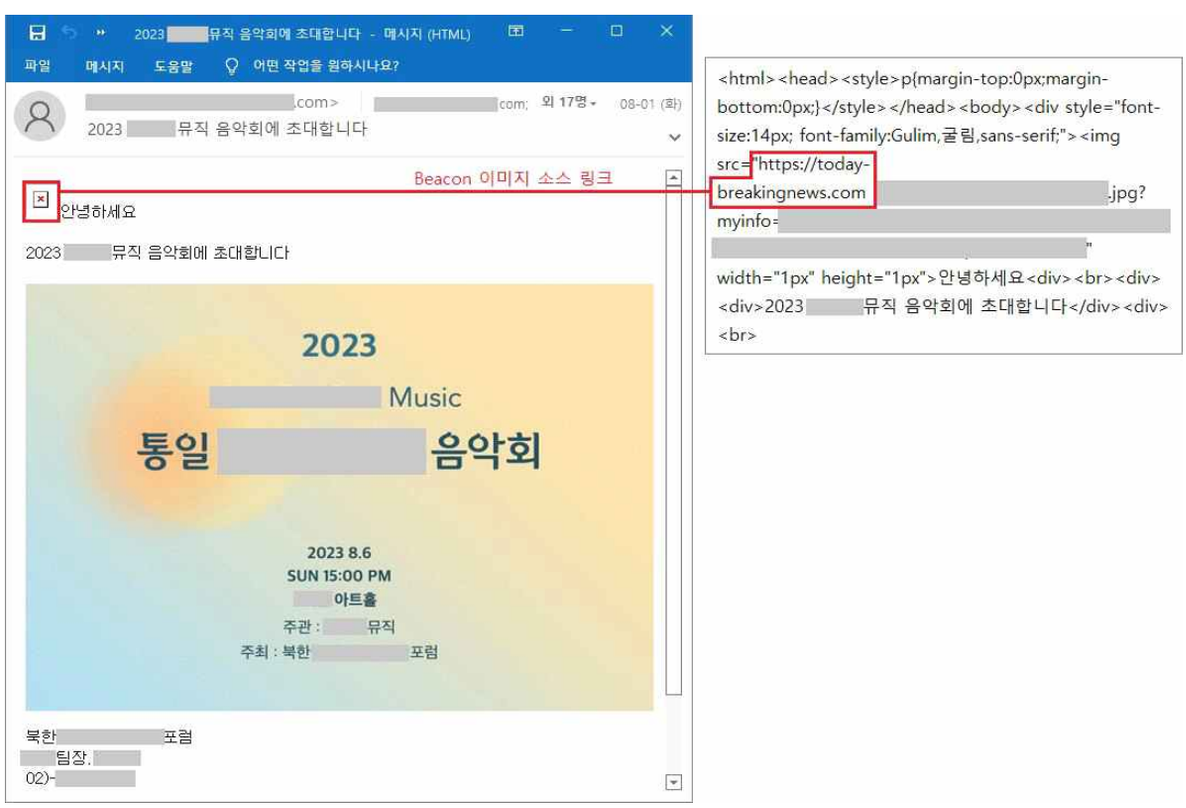
언론사명	(Sub) Domain 주소		IP 주소 (국가코드)
세계일보	공식	segye[.]com	[생략]
	피싱	segye.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
전자신문	공식	etnews[.]com	[생략]
	피싱	etnews.newspad[.]info	84.32.131[.]47 (LT) -
중앙일보	공식	joongang.co[.]kr	[생략]
	피싱	joongang.newspad[.]info	84.32.191[.]233 (LT) -
동아일보	공식	donga[.]com	[생략]
	피싱	donga.newspad[.]info	84.32.191[.]233 (LT) -

2) 통일 음악회 사칭 APT37 공격 유사 사례

2023년 8월 1일, 대북분야 종사자 및 탈북민 약 18명 상대로 통일 관련 음악회 초대로 사칭한 피싱 공격이 수행된다. 해당 이메일에는 악성 링크나 첨부 파일이 존재하지 않는다.

그러나 이메일 내부에 비콘용 호스트(today-breakingnews[.]com) 주소가 숨겨져 있어 수신자들이 해당 메일을 열람하는지 원격지에서 정찰하게 된다.

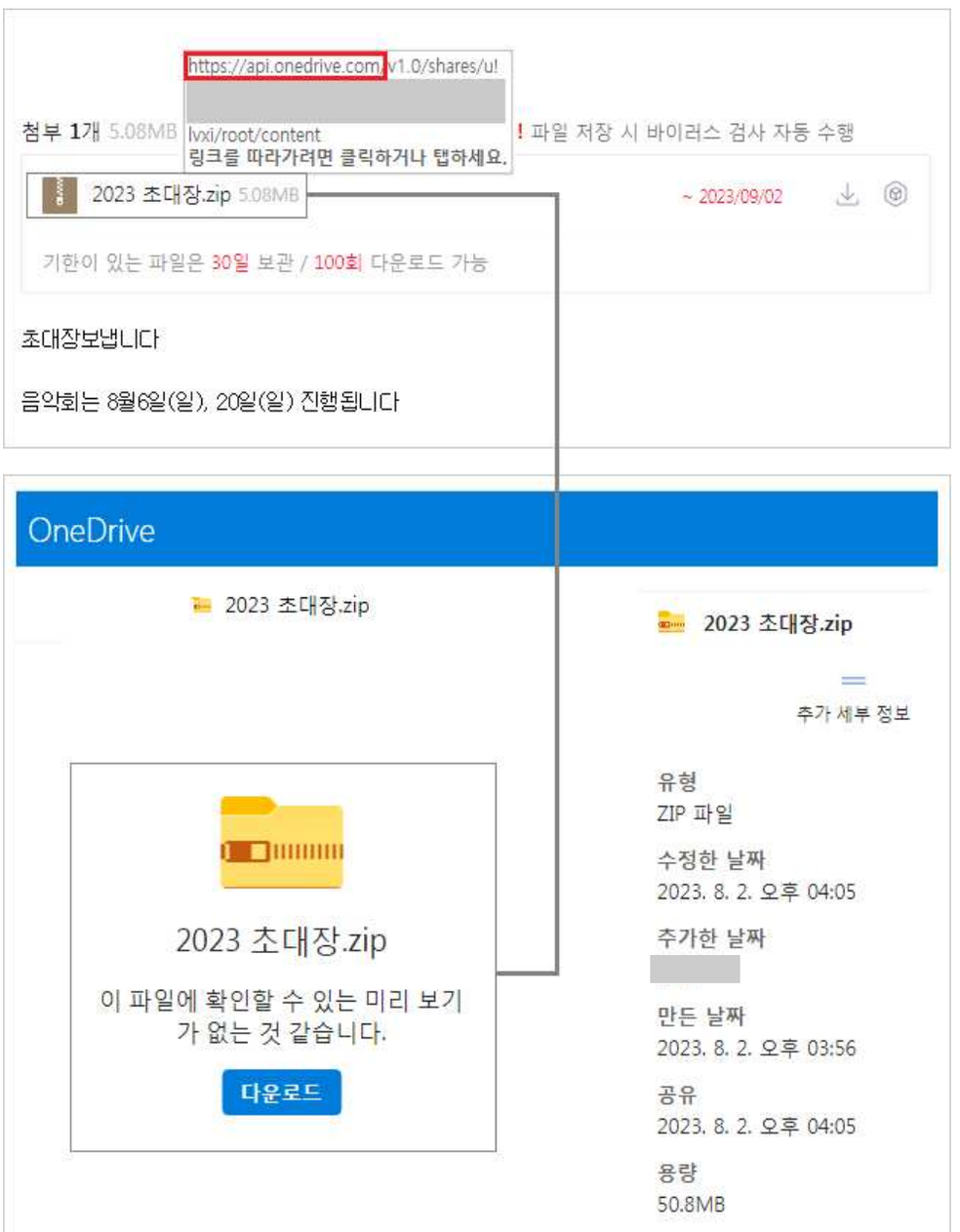
[그림 16] 통일 관련 음악회로 사칭해 현혹 중인 메일의 비콘 코드 화면



해당 이메일 수신자 중 음악회 초대에 현혹돼 추가 문의나 회신 등 반응을 보인 인물에게는 두번째 메일을 보내며, 악성 파일 링크를 삽입하게 된다.

마치 정식 초대장을 보내주는 것처럼 가장한 두번째 메일에는 '2023 초대장.zip' 첨부 파일이 원드라이브(OneDrive) 클라우드로 연결된 상태로 전송된다.

[그림 17] 음악회 초대장으로 위장한 해킹 이메일 화면



다운로드 된 압축 파일 내부에는 '2023 초대장.pdf.lnk' 이름의 바로가기 유형의 악성 파일이 포함되어 있다. LNK 악성 코드가 작동되면 내부에 포함된 Powershell 명령 등이 작동한다.

그 다음 공격자가 지정한 또 다른 원드라이브 클라우드 경로에서 마치 PDF 문서처럼 위장한 'homoa.pdf' 파일이 호출되는데, 이것은 암호화된 ROKRAT 변종 악성 파일로 메모리상에 파일리스 기반으로 작동하여 컴퓨터 정보를 피클라우드(pCloud)로 유출하게 된다.

본 사례에서 식별된 'today-breakingnews[.]com' 도메인은 BitB 피싱 공격의 비콘으로 쓰인 'naver.com[.]de' 도메인과 연결되는 '84.32.131[.]47' 아이피 주소 등과 정확히 연결된다.

선별한 몇 가지 케이스만 비교해 봐도, 전형적인 APT37 공격과 BitB 피싱이 직간접적으로 연결되고 있다는 것을 관찰할 수 있다.

5. 결론 및 대응방법 (Conclusion)

1) 실제 공식 행사 프로그램 사칭한 BitB 공격 등장

본 보고서는 실제 국내 특정인을 겨냥한 BitB 공격으로 평소 보안에 많은 관심과 경각심이 높은 이용자라도 정교한 피싱 공격에 현혹돼 노출될 가능성이 높은 유형으로 보다 각별한 주의가 필요하다.

거듭 강조하지만, BitB 공격 기술은 외관상 정상 URL 주소로 접속된 웹 브라우저 상태로 오인할 수 있기에 이곳에 기술된 내용뿐만 아니라, 앞으로 발생 가능한 유사 사례에 대한 적극적인 대비가 요구된다.

APT 공격이 날이 갈수록 지능화·고도화·다양화되고 있다. 국가배후 위협 행위자들은 거점 인프라 구축에 많은 자원과 비용을 투자하고 있어, 악성여부 판단 및 분석이 점차 어려워지는 추세이다.

2) BitB 피싱 공격 대응 방안

앞서 기술한 바와 같이, BitB 공격은 현재 이용 중인 웹 브라우저 화면상에 새로운 웹 브라우저 팝업화면처럼 정교하게 디자인한 새 창 화면을 띄우고, 이용자 로그인 정보를 입력하게 유도하는 절묘한 피싱 수법이다.

이때 보여지는 팝업창의 URL 주소는 공격자가 구성한 디자인으로 실제 공식 URL 주소를 임의로 삽입할 수 있기 때문에 육안상 정상 웹 사이트 주소와 동일하게 보여진다.

따라서 URL 주소만으로 진위여부를 판단하기 어렵다. 하지만, BitB 공격의 특성 상 새로 팝업 된 화면은 현재 이용 중인 웹 브라우저의 영역 밖으로 이동이 불가능하다. 그러므로, 로그인 정보 입력 창이 나타날 경우 우선 URL 주소의 정상 여부를 파악 후 웹 브라우저가 독립적으로 자유롭게 웹 브라우저 영역 밖으로 이동이 가능한지 따져보는 것만으로 BitB 피싱 피해를 최소화할 수 있다.

6. 침해 지표 (Indicator of Compromise)

1) 주요 MD5 Hash

- ec88f5b9e1b5947fd054a8cad89a6130
- 13e3405fc3ef62d4e2e3f5f19d9a9b53
- 51a82ce016de1c5d9c6e815b7d6d91b3

2) 연관된 명령제어(C2) 호스트 서버

- libertynorthkorea[.]org
- naver.com[.]de
- kakao.com[.]de
- hiworks.com[.]de
- samsunggalaxynote[.]com
- today-breakingnews[.]com
- daily-goodnews[.]com
- newspad[.]info
- attachmentfile[.]site
- mailstorage[.]site
- myfilestorages[.]com
- naveruser[.]com
- daumuser[.]net
- naver[.]one
- daum[.]uno
- kakao[.]uno
- kakaoserver[.]com
- kakaotalkwallet[.]com
- kakaocopyright[.]com
- navercopyright[.]com
- emailsecurity[.]autos
- daum.net[.]ph
- kakao.com[.]ph
- naver.com[.]pe
- mailcorp[.]services

- kakao.com[.]vc
- mail-setting[.]com
- naver.cn[.]com
- 141.164.54[.]9
- 38.54.94[.]241
- 84.32.131[.]47
- 84.32.191[.]233
- 5.199.168[.]70
- 5.199.168[.]240
- 45.61.137[.]22
- 45.61.138[.]203
- 45.61.139[.]99
- 45.61.139[.]138
- 45.61.158[.]17
- 162.33.179[.]79
- 168.100.11[.]133
- 172.86.96[.]38
- 192.153.57[.]154
- 193.149.176[.]233
- 206.166.251[.]146

7. 공격 지표 (Indicator of Attack)

1) MITRE ATT&CK[8] Matrix - APT37[9] Group Descriptions

[표 6] MITRE ATT&CK, Tactics and Techniques

Tactic	Technique	Description
Reconnaissance	T1598.002[10]	Phishing for Information: Spearphishing Attachment
	T1598.003[11]	Phishing for Information: Spearphishing Link
Resource Development	T1585.002[12]	Establish Accounts: Email Accounts
	T1585.003[13]	Establish Accounts: Cloud Accounts

8) https://attack.mitre.org/
9) https://attack.mitre.org/groups/G0067/
10) https://attack.mitre.org/techniques/T1598/002/

Tactic	Technique	Description
Initial Access	T1566.002[14]	Phishing: Spearphishing Link
	T1566.003[15]	Phishing: Spearphishing via Service

8. 참고 자료 (Reference)

[표 7] 참고 자료

연번	제목	출처
1	[Genians] 한국내 macOS 이용자를 노린 APT37 공격 등장	https://www.genians.co.kr/blog/threat_intelligence_report_macos
2	[Genians] 북한인권단체를 사칭한 APT37 공격 사례	https://www.genians.co.kr/blog/threat_intelligence_report_apt37
3	[mrd0x] Browser In The Browser (BITB) Attack	https://mrd0x.com/browser-in-the-browser-phishing-attack/
4	[zscaler] Fake Sites Stealing Steam Credentials	https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials

11) https://attack.mitre.org/techniques/T1598/003/
12) https://attack.mitre.org/techniques/T1585/002/
13) https://attack.mitre.org/techniques/T1585/003/
14) https://attack.mitre.org/techniques/T1566/002/
15) https://attack.mitre.org/techniques/T1566/003/

사이버보안 대연합 보고서

2023년 8월 31일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원

KISA 한국인터넷진흥원

kisia 한국정보보호산업협회