GSC-R230901-Rev-3.0

Distribution TLP : WHITE

위협 분석 보고서

한국 내 대북분야 종사자를 겨냥한 고도화된 BitB 공격 등장

2023. 09. 01

엔드포인트보안연구개발실

Genians Security Center

집필 : 문종현 센터장, 박경령 책임, 유 현 전임, 송관용 연구원

Genians

- 목차 (CONTENTS) -

◈ 주요 요약 (Executive Summary)

- 미국내 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

01. 개요 (Overview)

a. 국제 북한인권단체를 사칭한 위협 식별 (Threat Hunting)

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

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

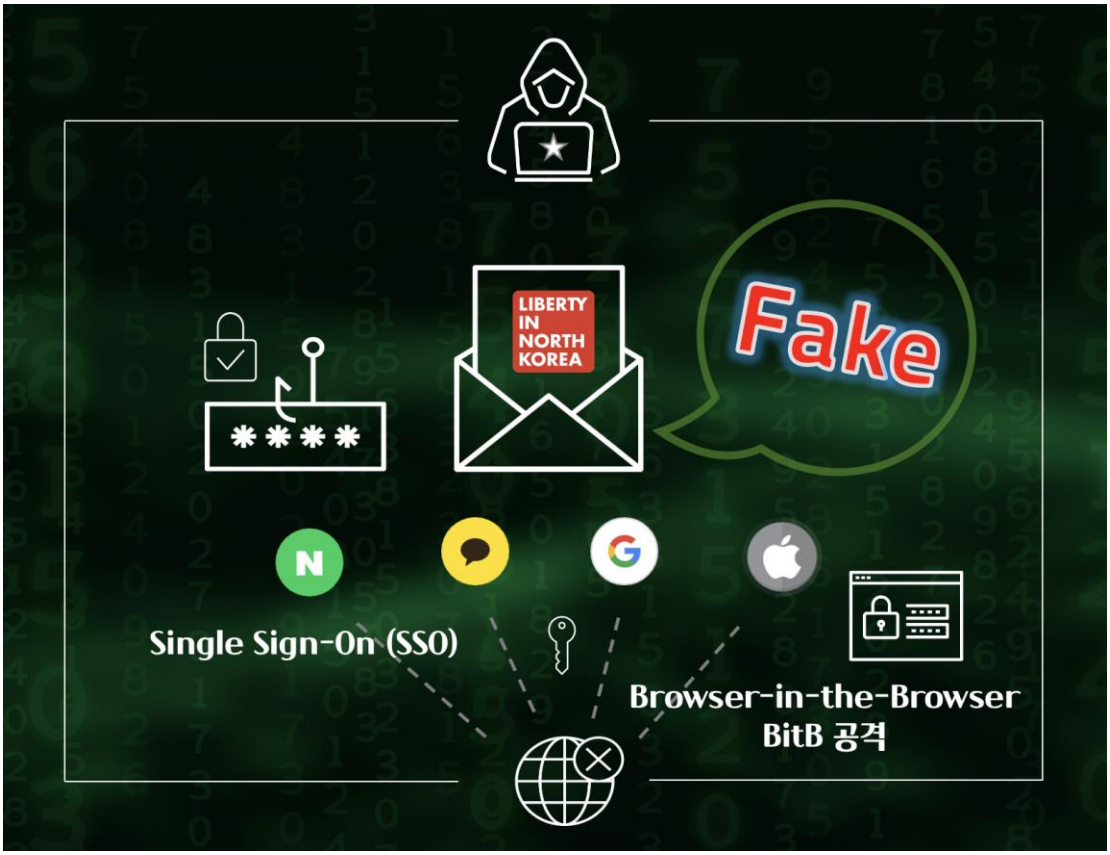
○ 해당 프로그램은 북한 출신 활동가를 대상으로 하고 있으며, 실제 지원 기한은 7 월 26 일로 공격이 확인된 24 일 기준 약 2 일의 여유가 있었습니다. 총 금액은 600 만원으로 매달 50 만원씩 12 개월간 활동 지원금을 제공하게 됩니다. 나름 촉박한 신청 기한을 감안한다면 공격 대상자를 현혹하는데 충분한 요소로 볼 수 있습니다.

○ 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 있습니다. 따라서 해당 위협은 탈북민이나 유관 단체가 주요 타깃에 해당될 수 있습니다.

b. 피싱 공격 흐름 (Phishing Attack Flow)

○ 본격적인 공격은 이메일내 상세 내용을 보려면 별도의 홈페이지 주소를 참고하라는 식으로 계정 해킹을 유인하는데, 실제 해당 프로그램에서 배포한 내용을 그대로 모방했습니다. 만약, 해당 내용에 속아 공격자가 직접 개설한 가짜 사이트로 연결되면, 피싱 공격이 진행됩니다.

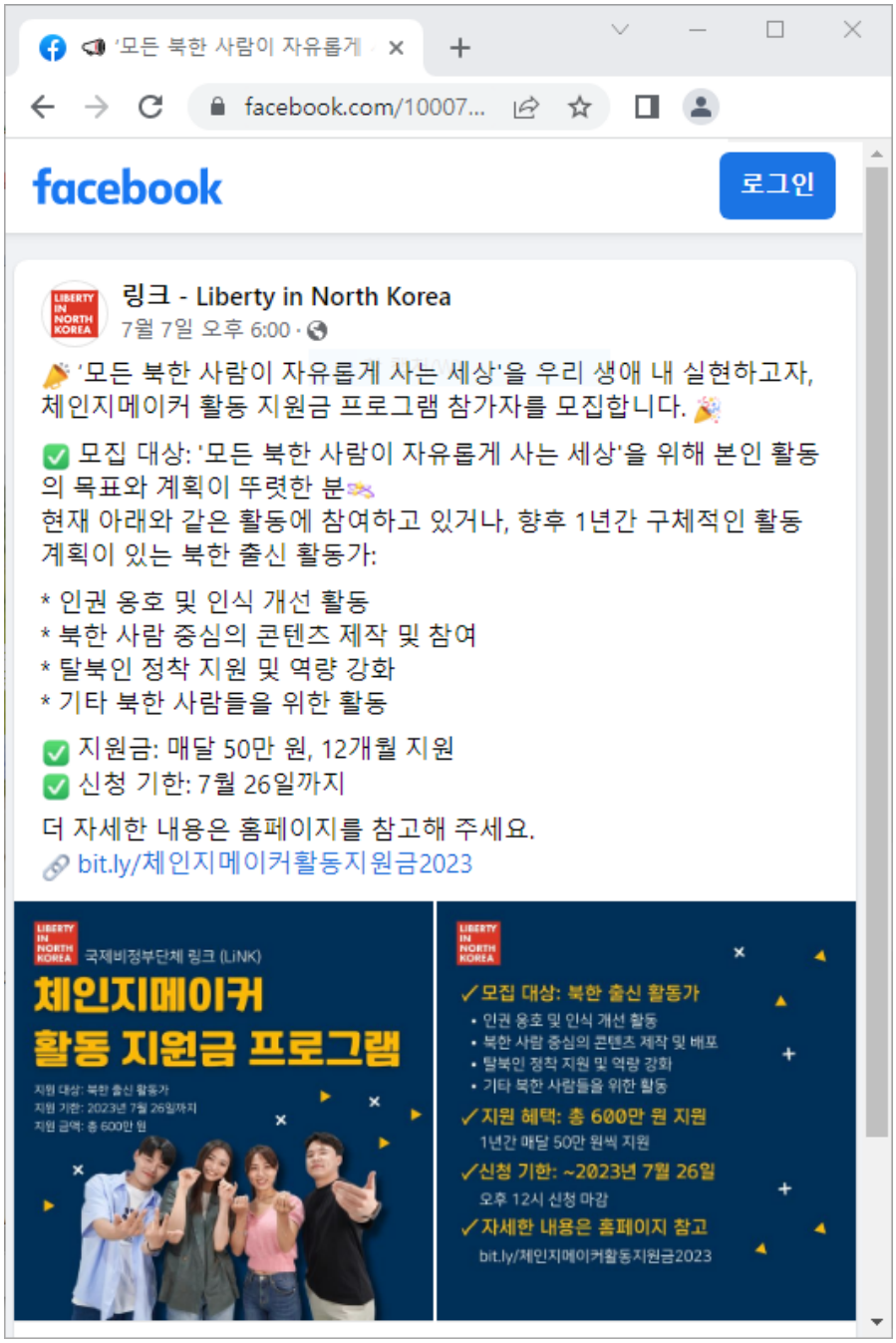
○ 마치 탈북민의 북한인권 활동 지원 프로그램처럼 조작된 피싱 이메일로 공격이 수행됩니다. 이메일 본문에 삽입된 가짜 홈페이지 주소에 접근할 경우 계정 탈취 목적의 피싱 사이트가 나타납니다. 이때 입력된 이메일 주소와 비밀번호가 공격자에게 유출되는 과정을 거칩니다.



[그림 01] 피싱 공격 간략 흐름도

c. 공격 전술 및 기술, 절차 (TTPs) & BitB 공격

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



[그림 02] 링크(LiNK) 단체 공식 페이스북 안내문 화면

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

○ 공격 거점으로 사용할 피싱용 도메인과 웹 서버를 직접 구축했고, 'Browser In The Browser(BitB)' 공격 기술을 사용했습니다.[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 중에 하나입니다.

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

○ GSC 는 본 피싱 공격이 BitB 공격 기술을 절묘하게 사용한 점에 주목했습니다. 이번 보고서 사례처럼 외관상 보여지는 URL 주소의 진위여부를 판단하는데 보다 세심한 주의와 관심이 필요한 이유입니다. 육안상 인지된 주소만을 믿고 접근해 함부로 개인정보를 입력할 경우 예기치 못한 위협에 노출될 가능성이 높습니다.

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

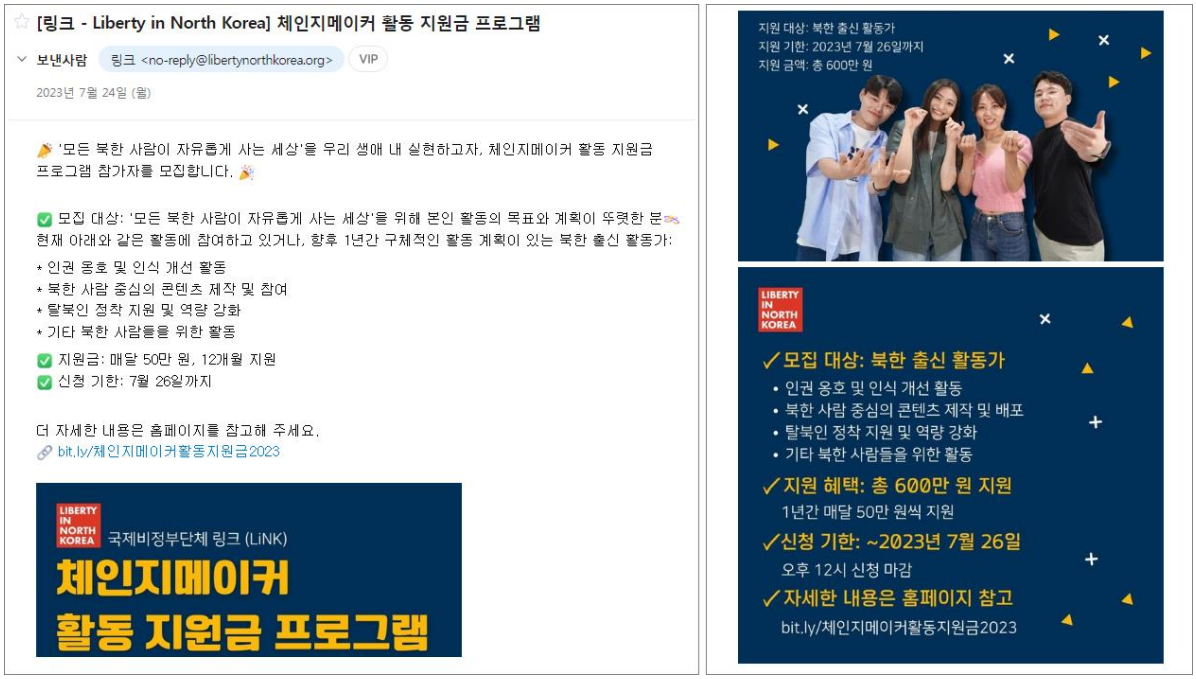
○ 더불어 본인이 사용하는 웹 브라우저의 유저 인터페이스(UI)와 일관된 디자인과 화면 모드를 유지하고 있느냐 비교하는 것입니다. 웹 브라우저의 버튼이나 아이콘 등 구성 디자인 요소에 차이점이 없는지 면밀히 비교해 보는 것입니다.

[1] SSO 란 무엇인가요? - Single Sign-On 설명 - Amazon AWS
[2] Browser In The Browser (BITB) Attack

02. 공격 시나리오 (Attack Scenario)

a. 초기 접근 단계-피싱 (Initial Access-Phishing)

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



[그림 03] 실제 공격에 사용된 이메일 화면

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

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

b. 피싱 메일 분석 (Phishing Email Analysis)

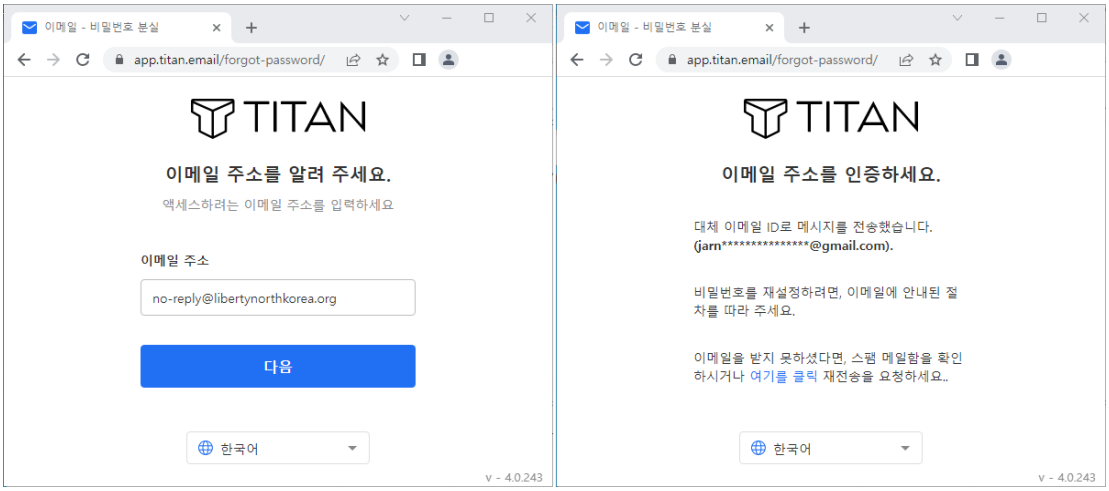
○ 공격자는 'titan[.]email' <(구)flockmail[.]com> 이메일 플랫폼 서비스를 악용해 피싱 공격을 수행합니다. 이 서비스를 활용한 공격은 북한 연계 해킹 조직이 종종 사용하고 있습니다.[3]

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

○ 흥미롭게도 코드쉐프는 국제 소프트웨어 프로그래밍 경진대회로 북한 김일성 종합대, 김책 공대 학생들이 지난 2013 년부터 경연에 참가해 수 차례 우승을 차지한 것으로 알려져 있습니다.[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 있습니다.[6]

[3] Flockmail (현재 Titan) 이메일 플랫폼
[4] 바빈 투라키아 (위키디피아)
[5] 北 사이버전사 국제 프로그래밍 대회 휩쓸어 (월간조선)
[6] 北 해커가 세계대회 휩쓰는 이유 (한국경제)



[그림 04] 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 있습니다. 자세히 보면, 영문 알파벳 R 과 N 을 소문자로 연이어 사용한 전형적 패턴을 볼 수 있는데, 보통 m 문자처럼 보이기 위한 수법입니다.

○ 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' 입니다.

```
=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?=
```

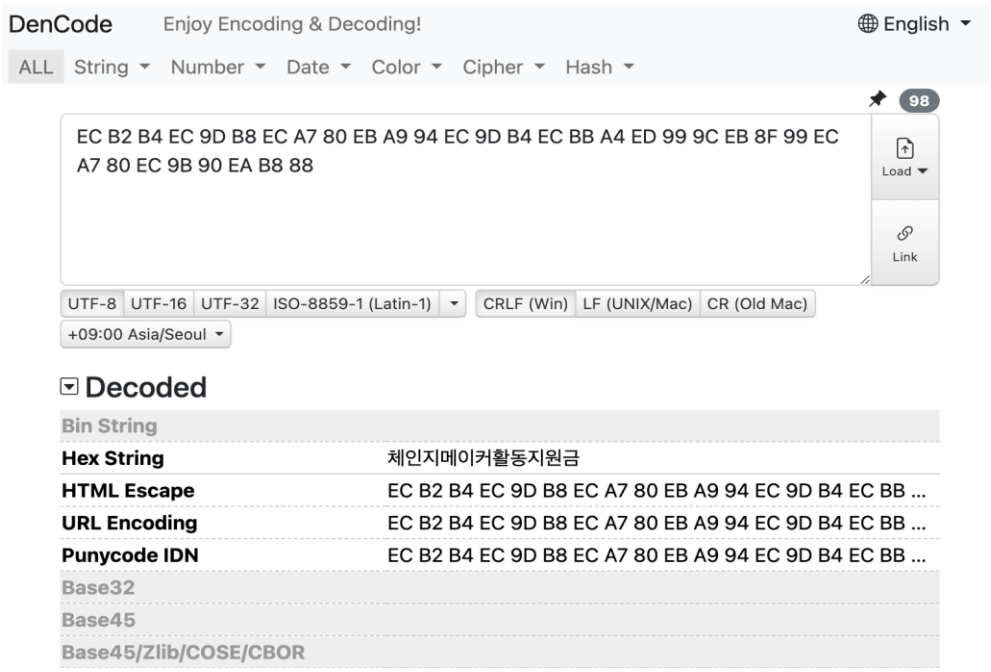
[그림 05] 이메일 내부에 숨겨져 있는 비콘 코드 화면

○ 웹 비콘 상단에 위치한 피싱 링크(bit.ly/체인지메이커활동지원금 2023) 주소는 한글 표기가 포함돼 있고, UTF-8 데이터가 포함돼 있습니다. 해당 코드는 DenCode 사이트에서 한글로 쉽게 변환이 가능합니다.[7]

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

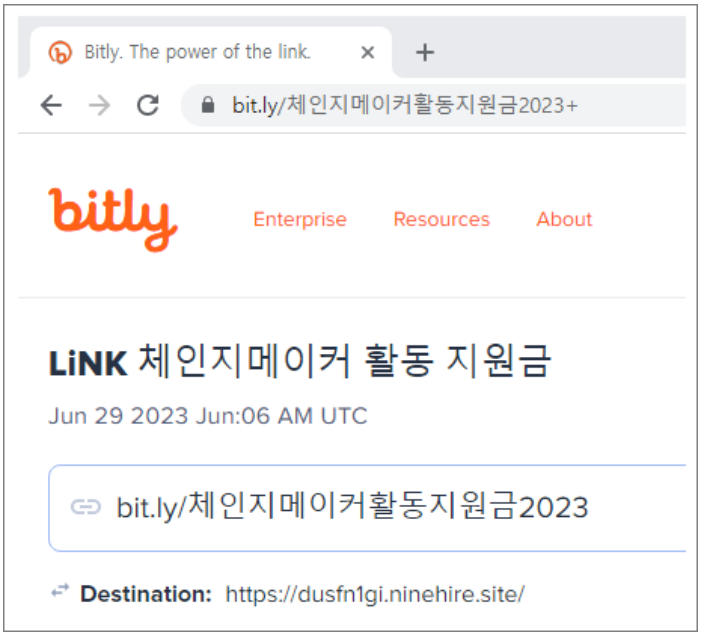
[표 01] 피싱 링크로 사용된 데이터 화면

[7] DenCode 데이터 변환 서비스



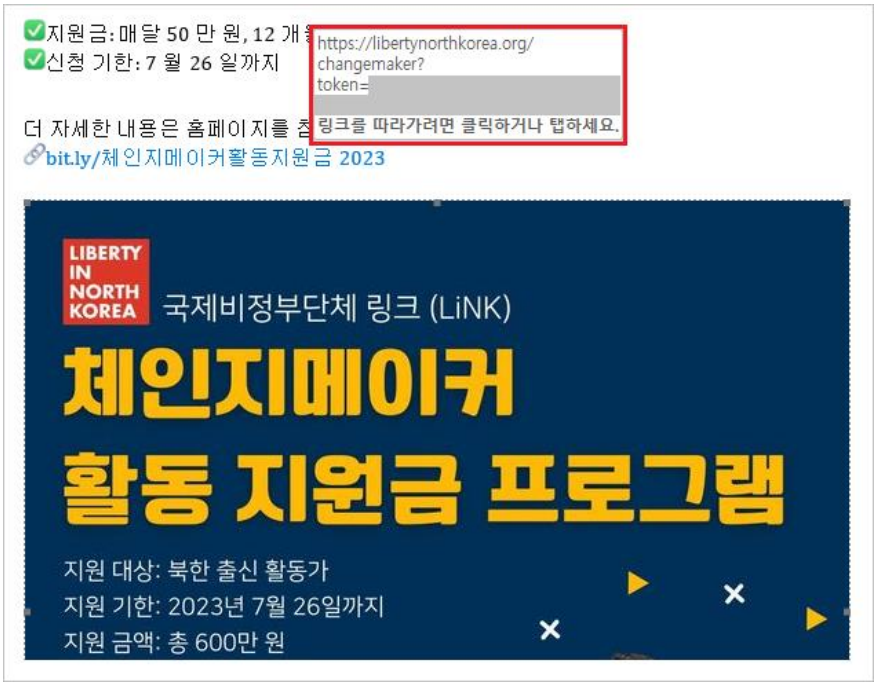
[그림 06] DenCode 서비스로 변환된 한글 문자열 화면

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



[그림 07] 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 회피합니다.

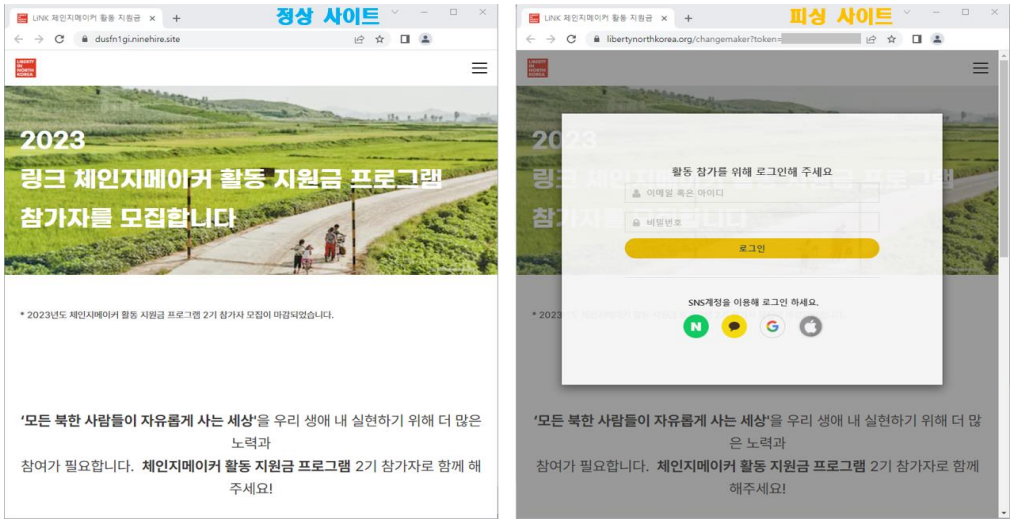


[그림 08] 해킹 이메일에 쓰인 단축 URL 주소 화면

03. 피싱 위협 분석 (Phishing Threat Analysis)

a. 정교한 유사 웹 사이트 구축

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



[그림 09] 정상 사이트(좌)와 피싱 사이트(우) 비교 화면

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

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

[표 02] 피싱 사이트의 아이프레임 코드 화면

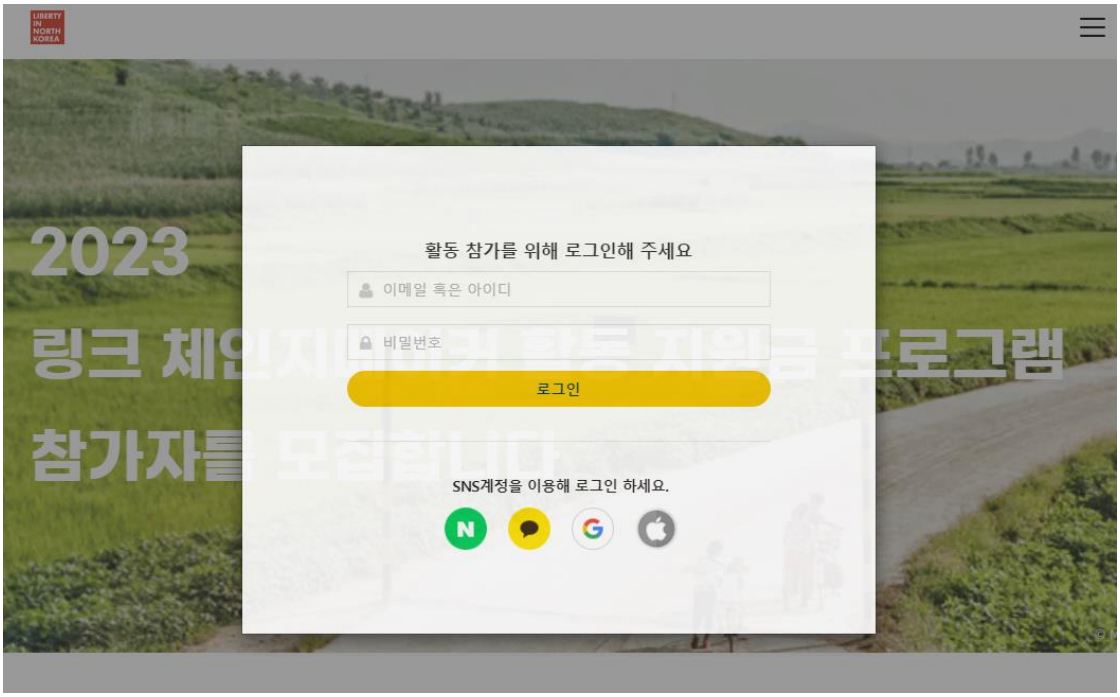
b. BitB 피싱 공격 기술

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

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

[표 03] 공식 사이트와 피싱 사이트 도메인 비교

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



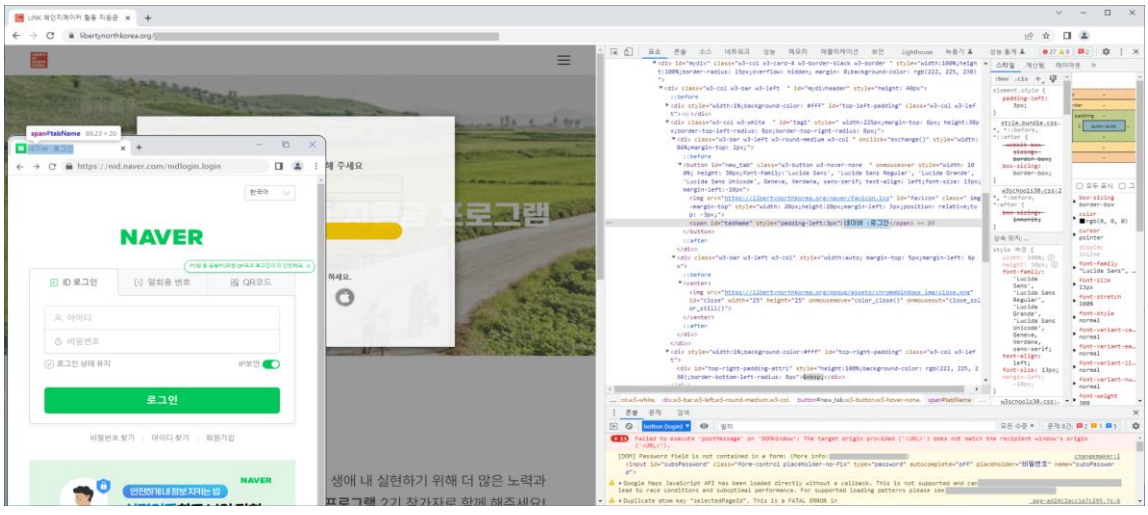
[그림 10] 피싱 사이트 접근 시 보여지는 팝업 창 화면

○ 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 방식입니다.

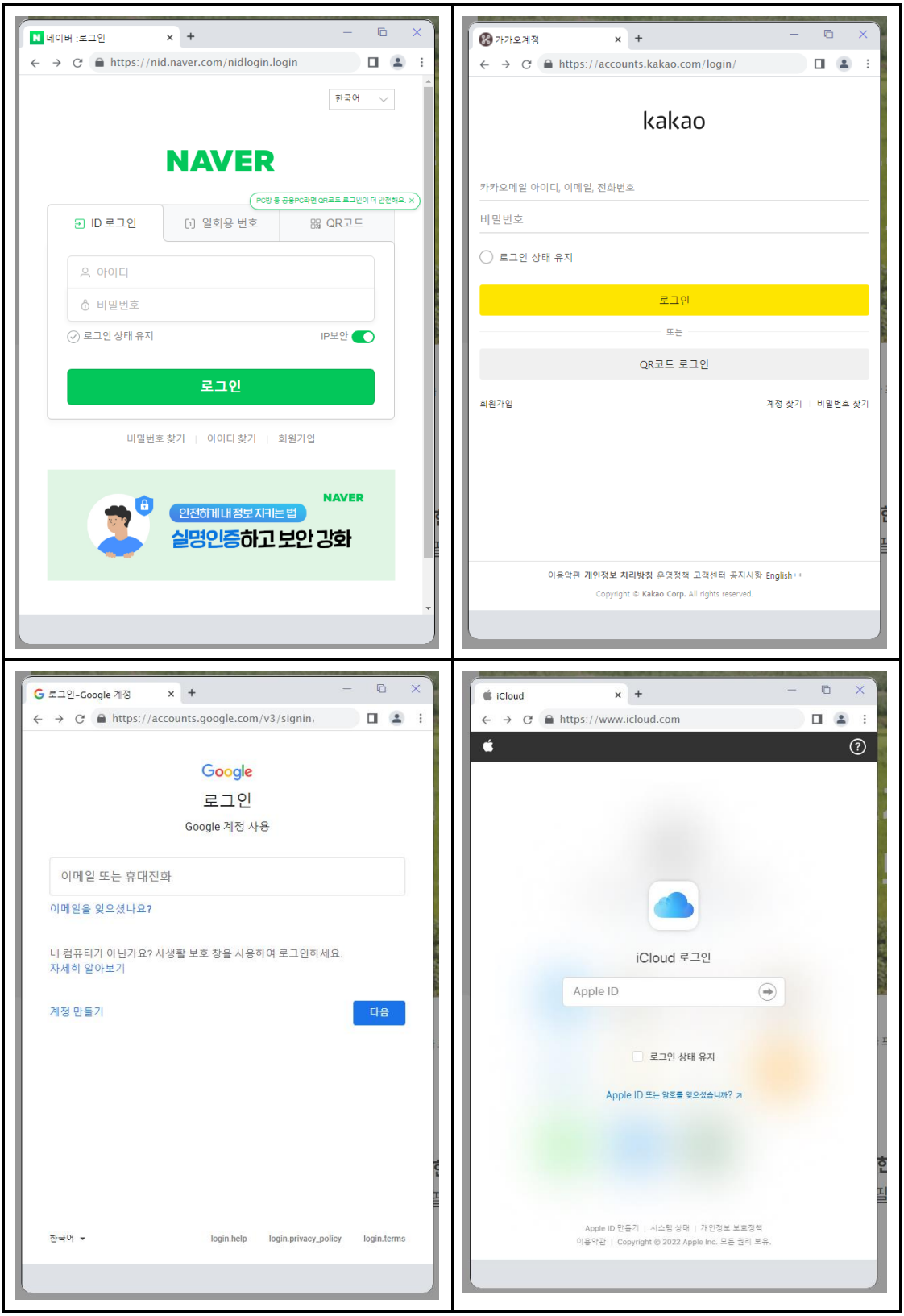
○ SSO 통합적 단일 인증 방식은 번거로운 별도의 가입절차가 없어 편의상 많이 쓰이고 있습니다. 평소 접해 보지 못한 생소한 웹 사이트에 신규로 가입하거나 로그인하는 것은 보안상 매우 조심스러운 부분입니다. 일반적으로 악성 의심 사이트를 구별하는데 있어, 절차상 가장 우선시되는 점은 웹 브라우저상 접속 주소 일 것입니다. 주소창에 보이는 인터넷 URL 경로가 내가 기존에 잘 알고 있던 도메인이라면 충분히 신뢰하고 로그인을 진행할 것입니다.

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

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



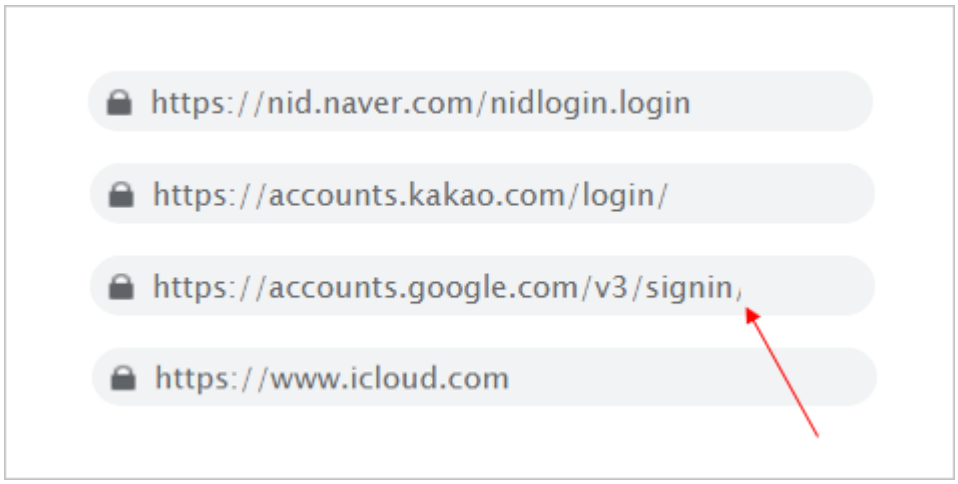
[그림 11] 가짜 로그인 팝업 창과 내부 코드 화면



[표 04] BitB 기법의 피싱용 팝업 창 화면 비교

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

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

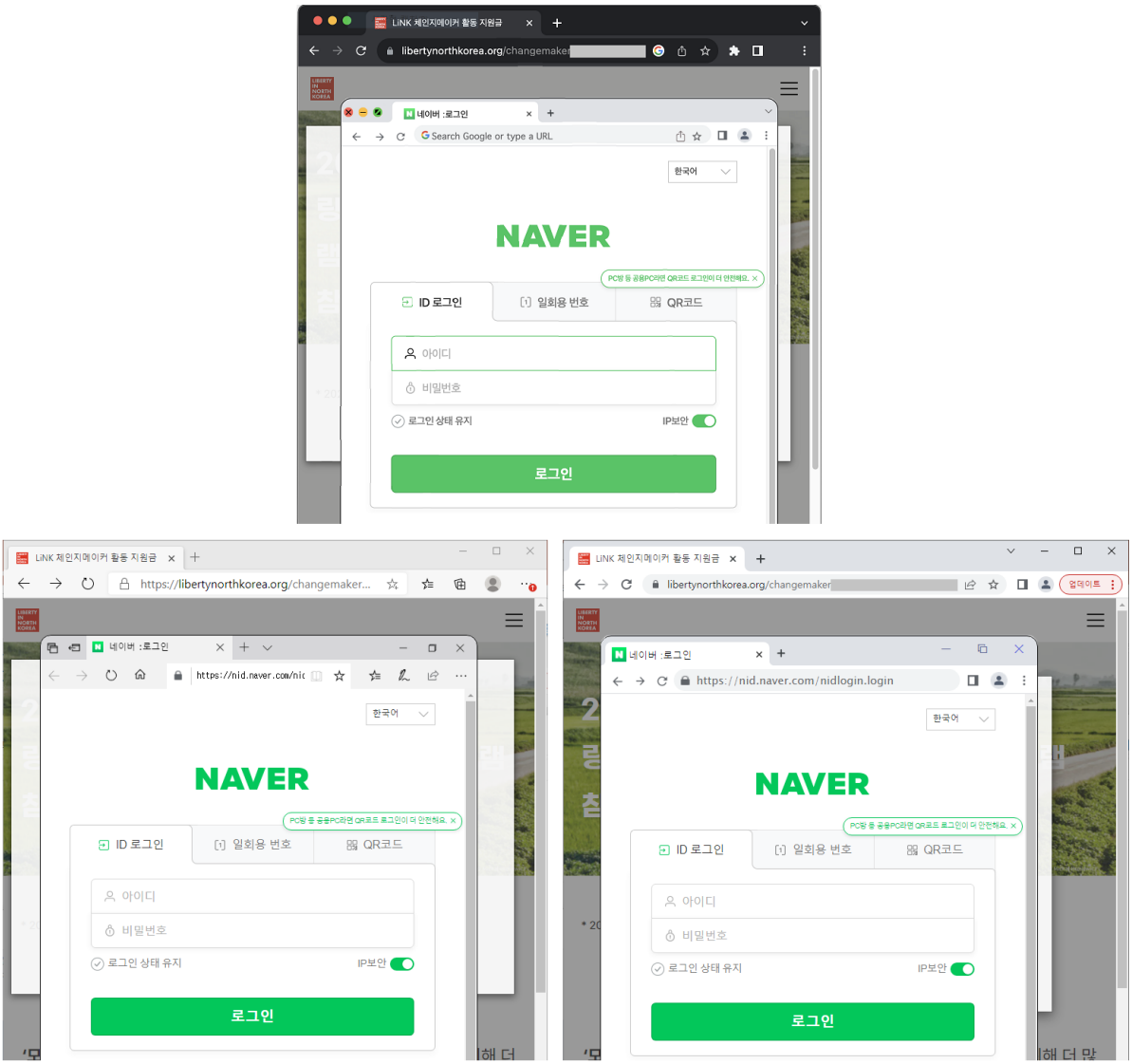


[그림 12] BitB 피싱 로그인 창 화면의 디자인된 URL 주소 화면

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

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

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



[그림 13] OS 및 웹 브라우저별 비교 화면

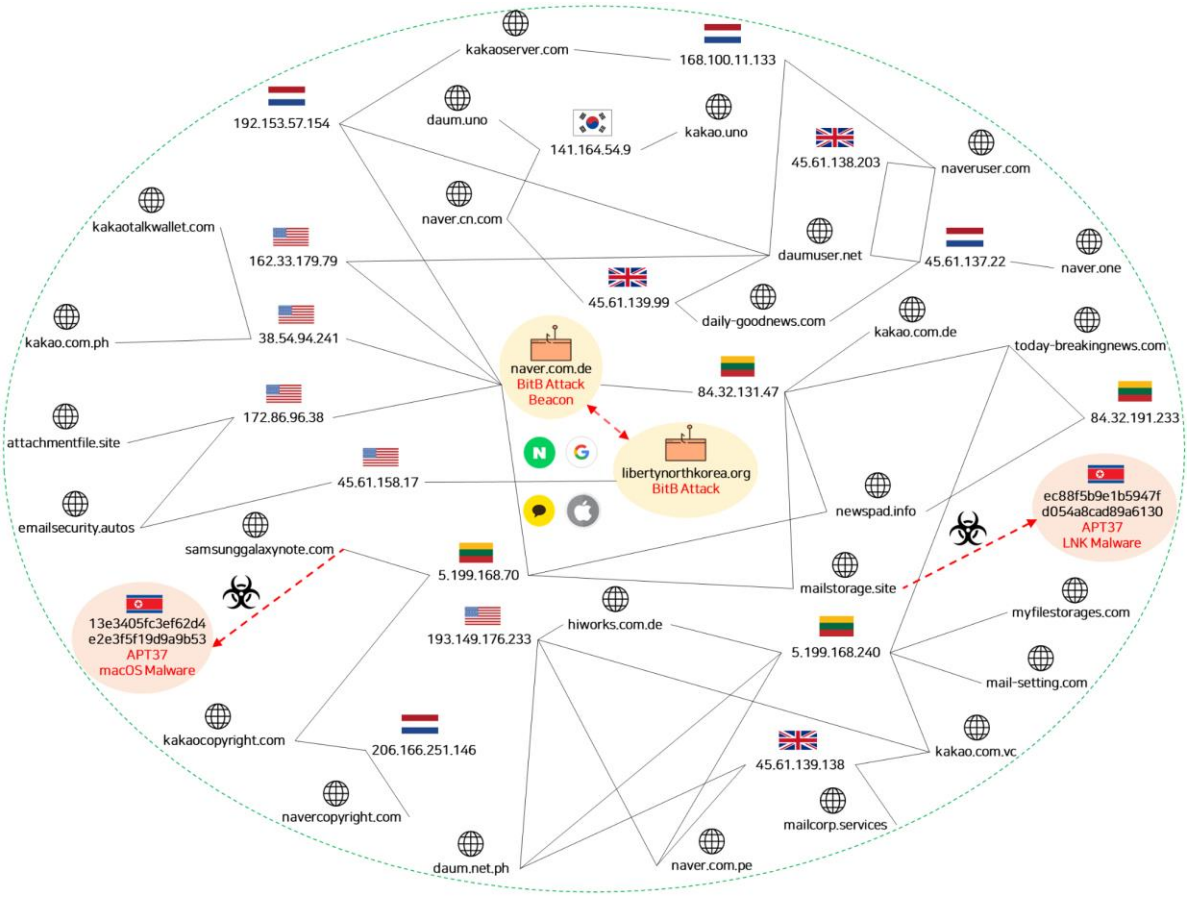
○ BitB 공격 여부를 가장 쉽고 정확하게 확인하는 방법은 팝업 창이 현재 사용 중인 웹 브라우저 영역 밖으로 이동이 가능한지를 보는 것입니다. BitB 피싱의 경우 팝업 창 자체가 단순히 별도의 웹 브라우저처럼 디자인으로 위장된 것이지 완전히 독립된 상태가 아닙니다. 따라서 기존 웹 브라우저 내에서만 이동이 가능한 고유한 특성을 활용한 방안이 있습니다.

04. 위협 인프라 유사도 (Similarity)

a. BitB 피싱과 APT37 공격 거점의 연결 고리

○ GSC 는 BitB 공격에 활용된 위협 지표를 조사하는 과정에서 APT37 공격 인프라와 연결된 고리를 찾았습니다.

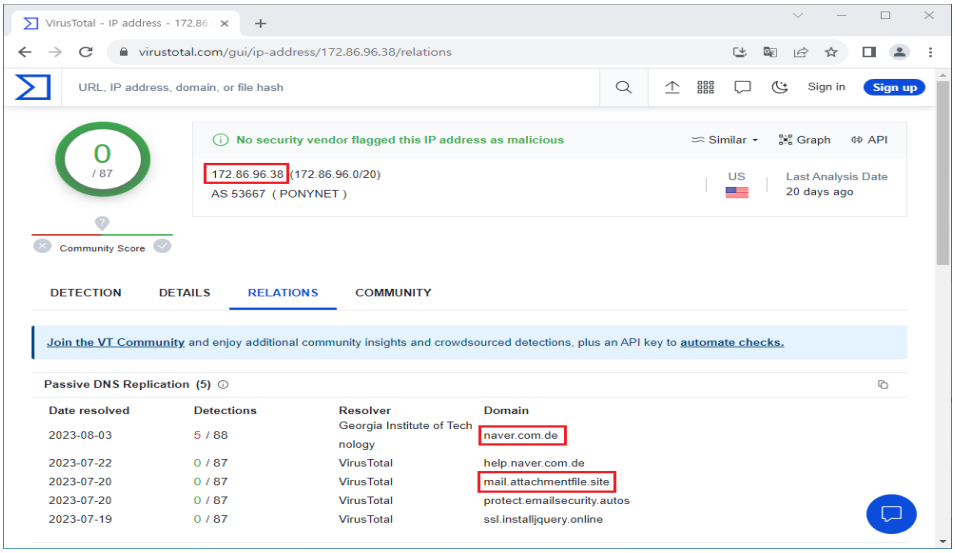
○ 이번 BitB 피싱 공격에 활용된 'libertynorthkorea[.]org' 도메인은 분석 시점 당시 미국 아이피 '45.61.158[.]17' 주소로 연결됐으며, 'ru.emailsecurity[.]autos' 도메인도 동일한 아이피가 사용됐습니다. 서브 도메인 중 'protect.emailsecurity[.]autos' 주소가 존재하며, '172.86.96[.]38' 주소로 연결됩니다.



[그림 14] BitB 공격 도메인과 APT37 공격 연관성 화면

○ ‘172.86.96[.]38’ 아이피에 연결됐던 Passive DNS 이력을 조회해 보면, 마치 국내 포털 사처럼 위장된 ‘naver.com[.]de’ 도메인이 사용된 기록을 확인할 수 있습니다. 참고로 여기서 언급된 Passive DNS 란, 특정 (악성) 도메인이 DNS 쿼리를 통해 IP Lookup 된 휘발성 히스토리를 누적해 기록해 둔 것으로, 특정 기간 동안 이뤄지는 네트워크 위협 활동을 조사하는데 의미 있는 위협 인텔리전스 정보로 활용됩니다.

○ 이렇게 확인된 ‘naver.com[.]de’ 도메인의 경우, 앞서 설명된 해킹메일 본문내 숨겨진 비콘 도메인과 동일한 것을 볼 수 있습니다. 단순 우연으로 위협 인프라가 오버랩 된 것이 아니라, 계획적으로 활용됐을 가능성이 높은 이유입니다.



[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 사용됐습니다. 특히, 국내 언론사 웹 사이트처럼 위장한 ‘newspad[.]info’ 도메인의 서브 주소가 대표입니다.

○ ‘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 곳입니다.

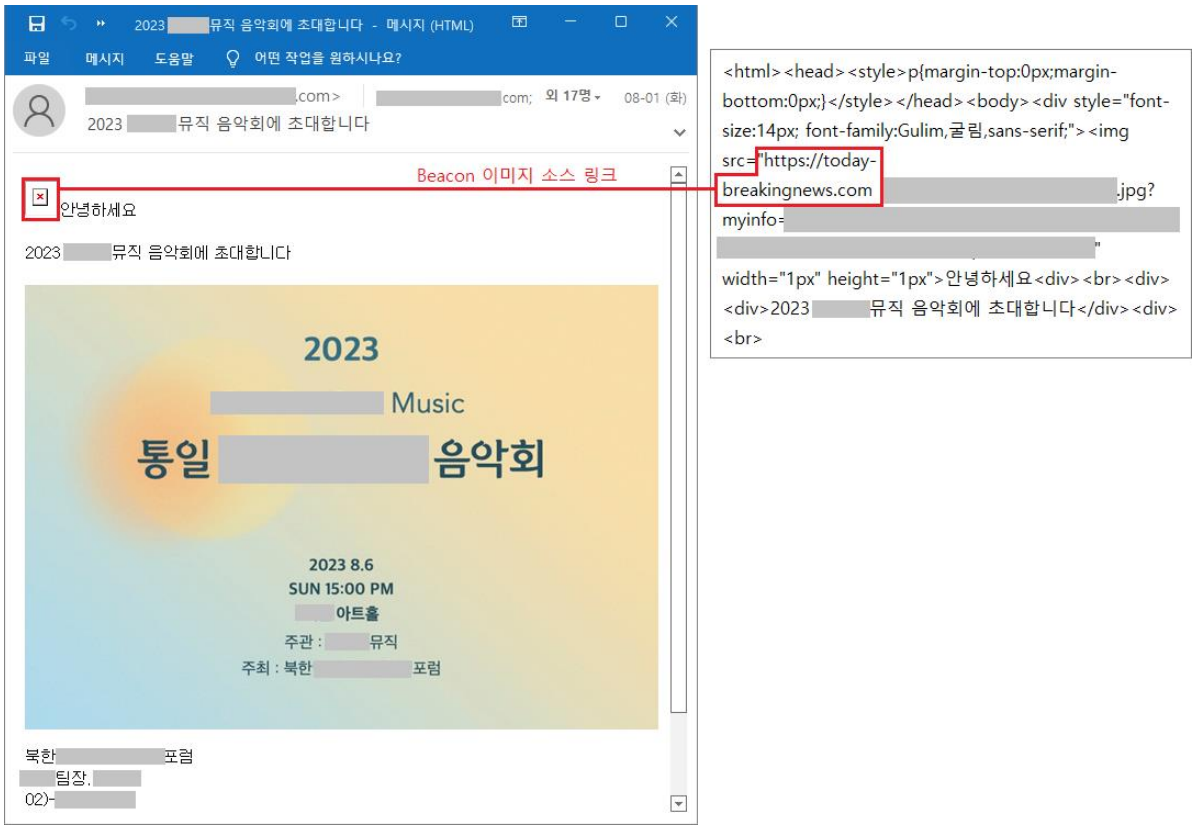
언론사명	(Sub) Domain 주소		IP 주소 (국가코드)
뉴데일리	공식	newdaily.co[.]kr	[생략]
	피싱	newdaily.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
조선일보	공식	chosun[.]com	[생략]
	피싱	chosun.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70 (LT)
국민일보	공식	kmib.co[.]kr	[생략]
	피싱	kmib.newspad[.]info	84.32.131[.]47 (LT) 5.199.168[.]70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

[표 05] 언론사 도메인으로 위장한 침해지표 비교 화면

b. 통일 음악회 사칭 APT37 공격 유사 사례

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

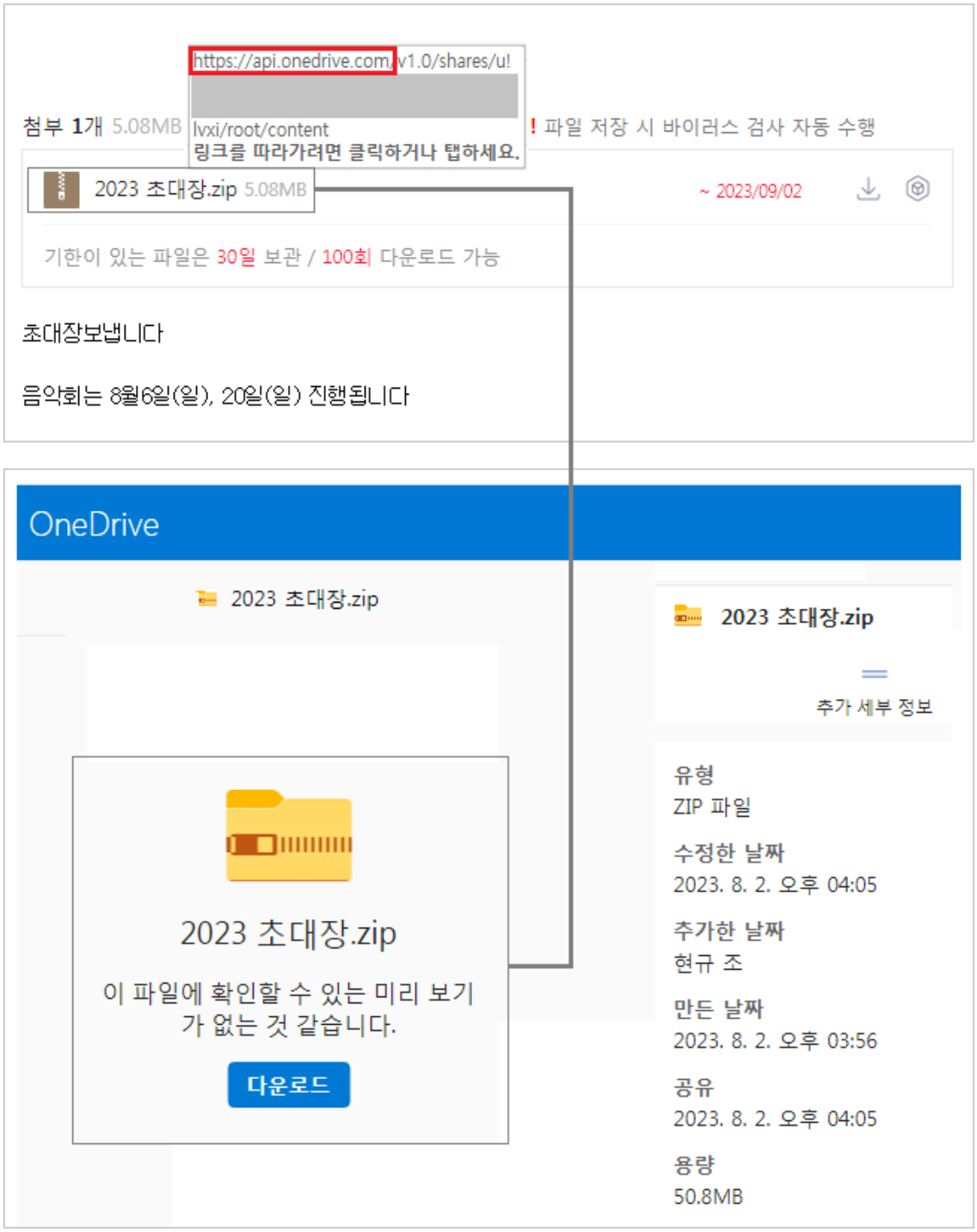
○ 그러나 이메일 내부에 비콘용 호스트(today-breakingnews[.]com) 주소가 숨겨져 있어 수신자들이 해당 메일을 열람하는지 원격지에서 정찰하게 됩니다.



[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 됩니다.

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



[그림 17] 음악회 초대장으로 위장한 해킹 이메일 화면

○ 다운로드 된 압축 파일 내부에는 '2023 초대장.pdf.lnk' 이름의 바로가기 유형의 악성 파일이 포함돼 있습니다. LNK 악성 코드가 작동되면 내부에 포함된 Powershell 명령 등이 작동합니다.

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

○ 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 연결됩니다.

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

05. 결론 및 대응방법 (Conclusion)

a. 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 필요합니다.

○ 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 요구됩니다.

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

b. BitB 피싱 공격 대응 방안

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

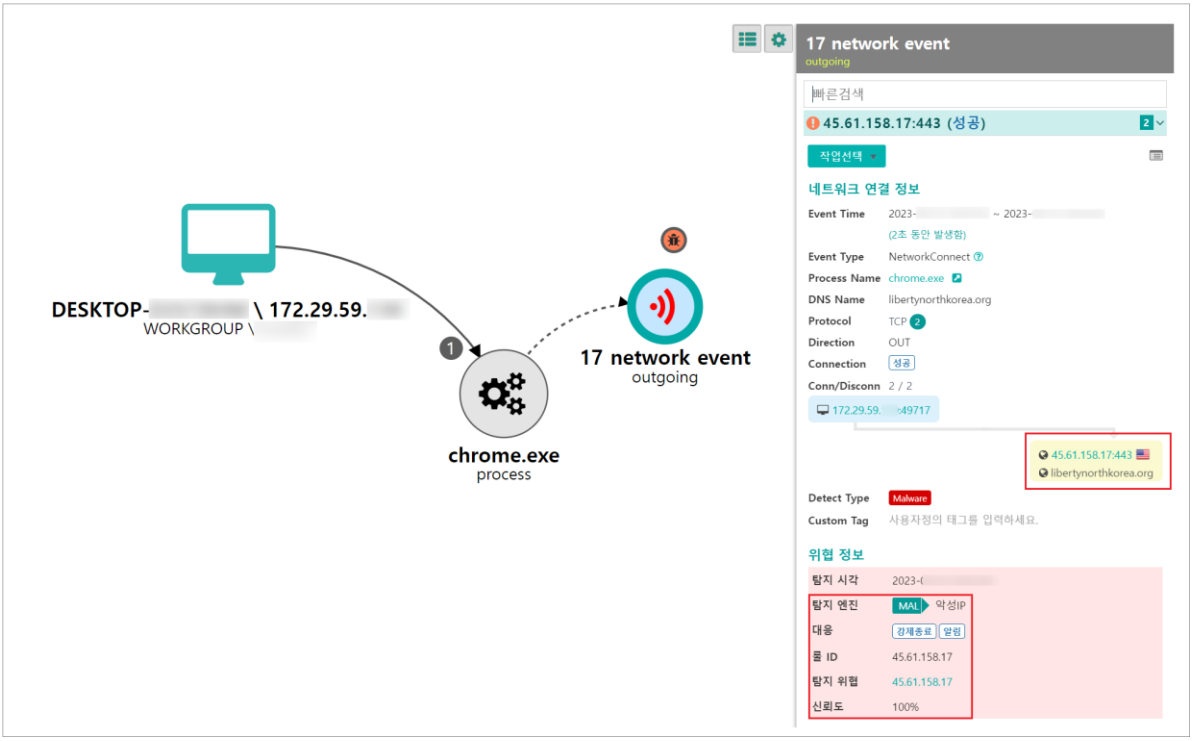
○ 이때 보여지는 팝업창의 URL 주소는 공격자가 구성한 디자인으로 실제 공식 URL 주소를 임의로 삽입할 수 있기 때문에 육안상 정상 웹 사이트 주소와 동일하게 보여집니다.

○ 따라서 URL 주소만으로 진위여부를 판단하기 어렵습니다. 하지만, BitB 공격의 특성 상 새로 팝업 된 화면은 현재 이용 중인 웹 브라우저의 영역 밖으로 이동이 불가능합니다. 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 있습니다.

c. Genian EDR 제품을 통한 효과적인 대응

○ 공개된 위협 분석 보고서나 OSNIT 침해지표(IoC) 중 우선 순위 및 관리 권한에 따라 탐지 대응이 필요한 악성 IP 주소가 존재할 수 있습니다.

○ Genian EDR[8] 운영 환경에 악성 IP '45.61.158[.]17' 주소가 추가된 경우, BitB 피싱 사이트 'libertynorthkorea[.]org' 도메인에 접근할 경우 신속하게 탐지 및 대응이 가능합니다. 더불어 시각화 기능을 통해 조기에 위협을 조사할 수 있습니다.



[그림 18] Genian EDR 제품에서 피싱 IP 주소를 탐지 대응 화면

[8] https://www.genians.co.kr/products/genian-edr/

○ 엔드 포인트에서 악성 IP 주소가 탐지된 경우, 실시간 위협 관리 내용을 통해 각 이벤트 시간 및 요약 내용을 보안 담당자가 편리하게 확인할 수 있습니다. 이를 통해 정확한 분석과 침해사고 조사에 도움을 얻을 수 있습니다.

이벤트 시각	탐지	이벤트	이벤트 요약
2023-		NetworkConnect	chrome.exe 프로세스가 maps.googleapis.com 로 UDP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 t1.daumcdn.net 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 dusfn1gi.ninehire.site 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 ssl.installjquery.online 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 r3.i.lencr.org 로 TCP : Outgoing 통신을 했습니다.
2023-	●	NetworkConnect	chrome.exe 프로세스가 libertynorthkorea.org 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 update.googleapis.com 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 update.googleapis.com 로 UDP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 www.google.com 로 UDP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 www.google.com 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 www.google.com 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 accounts.google.com 로 TCP : Outgoing 통신을 했습니다.
2023-		NetworkConnect	chrome.exe 프로세스가 clientservices.googleapis.com 로 TCP : Outgoing 통신을 했습니다.
2023-		ProcessStart	chrome.exe 프로세스에 의해 chrome.exe 프로세스가 시작되었습니다.

[그림 19] Genian EDR 기능을 통한 이벤트 분석 화면

○ 기관 및 기업내 보안 관리자는 이번 사례처럼 BitB 공격 등 지능화된 피싱 공격에 활용된 의심도 높은 해외 IP 대역 범위를 Genian EDR 탐지 정책에 우선 반영해 내부 침해사고를 선제적으로 관제 식별해 맞춤 대응 정책 및 방안을 수립하는데 활용할 수 있습니다.

06. 침해 지표 (Indicator of Compromise)

a. 주요 MD5 Hash

- ec88f5b9e1b5947fd054a8cad89a6130
- 13e3405fc3ef62d4e2e3f5f19d9a9b53
- 51a82ce016de1c5d9c6e815b7d6d91b3

b. 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

07. 공격 지표 (Indicator of Attack)

a. MITRE ATT&CK[9] Matrix - APT37[10] Group Descriptions

Tactic	Technique	Description
Reconnaissance	T1598.002	Phishing for Information: Spearphishing Attachment
	T1598.003	Phishing for Information: Spearphishing Link
Resource Development	T1585.002	Establish Accounts: Email Accounts
	T1585.003	Establish Accounts: Cloud Accounts
Initial Access	T1566.002	Phishing: Spearphishing Link
	T1566.003	Phishing: Spearphishing via Service

[표 06] MITRE ATT&CK, Tactics and Techniques

[9] ATT&CK : The Adversarial Tactics, Techniques, and Common Knowledge
[10] APT37 Group

08. 참고 자료 (Reference)

- 한국내 macOS 이용자를 노린 APT37 공격 등장 [Genians]
- 북한인권단체를 사칭한 APT37 공격 사례 [Genians]
- Browser In The Browser (BITB) Attack [mrd0x]
- Fake Sites Stealing Steam Credentials [zscaler]