북한 시장 물가 분석 문서 등으로 위장된 공격 사례

genians.co.kr/blog/market

Genians

◈ 주요 요약 (Executive Summary)

● LNK, HWP, HWPX, XLSX, DOCX 등 다양한 타입의 악성 파일을 이용한 공격 탐지
● [APT37] 그룹의 'LNK' 기반 공격의 연장선으로 사용 됨과 동시에 보안 취약점 결합
● 작년 이태원 사고 대처상황 문서로 위장한 'CVE-2022-41128' 취약점 공격의 연장선
● Genian EDR 기반으로 한 알려지지 않은 취약점 공격 탐지 및 신속한 위협 식별 요구

1. 개요 (Overview)

1.1. 배경 (Background)

○ 지니언스 시큐리티 센터(이하 GSC)는 HWP, HWPX 기반의 새로운 유형의 APT37 공격 징후를 다수 포착했습니다. 이 공격은 지난 2023년 5월 전후부터 11월까지 계속 이어졌으며, 주로 한국에서 쓰이는 HWP 한글 문서에 악의적 '오브젝트 연결 삽입'(OLE)을 활용한 공격입니다. APT37 HWP 공격과 더불어 Kimsuky HWP 공격 분석 내용은 11월달 지니언스 보고서를 통해 참고할 수 있습니다.[1]

○ 공격자는 HWP 파일 내부에 삽입한 OLE를 통해 공격자가 지정한 명령제어(C2) 서버로 연결을 시도하는데, 이때 연결된 사이트에서 Exploit 명령이 호출되는 과정을 거칩니다. 이번 보고서는 과거 캠페인과 최신 공격에서 관찰된 도구, 전술 및 절차(TTPs)를 다루는 포괄적인 분석을 제공하며, 한국에서 발생 중인 실제 위협 기반 인사이트 제공을 목적으로 합니다.

○ 본 위협 케이스는 보통의 HWP 확장자 뿐만 아니라 한컴에서 표준문서 형식으로 사용을 권장 중인 HWPX 포맷도 공격에 악용됐습니다. 한컴 홈페이지 FAQ 자료에 따르면, HWPX는 한글(HWP)문서의 콘텐츠를 표현할 수 있는 OWPML(개방형 워드프로세서 마크업 언어)로 개발된 파일형식으로 국가표준(KSX6101)으로 등록되어 있는 개방형 문서 포맷입니다.[2]

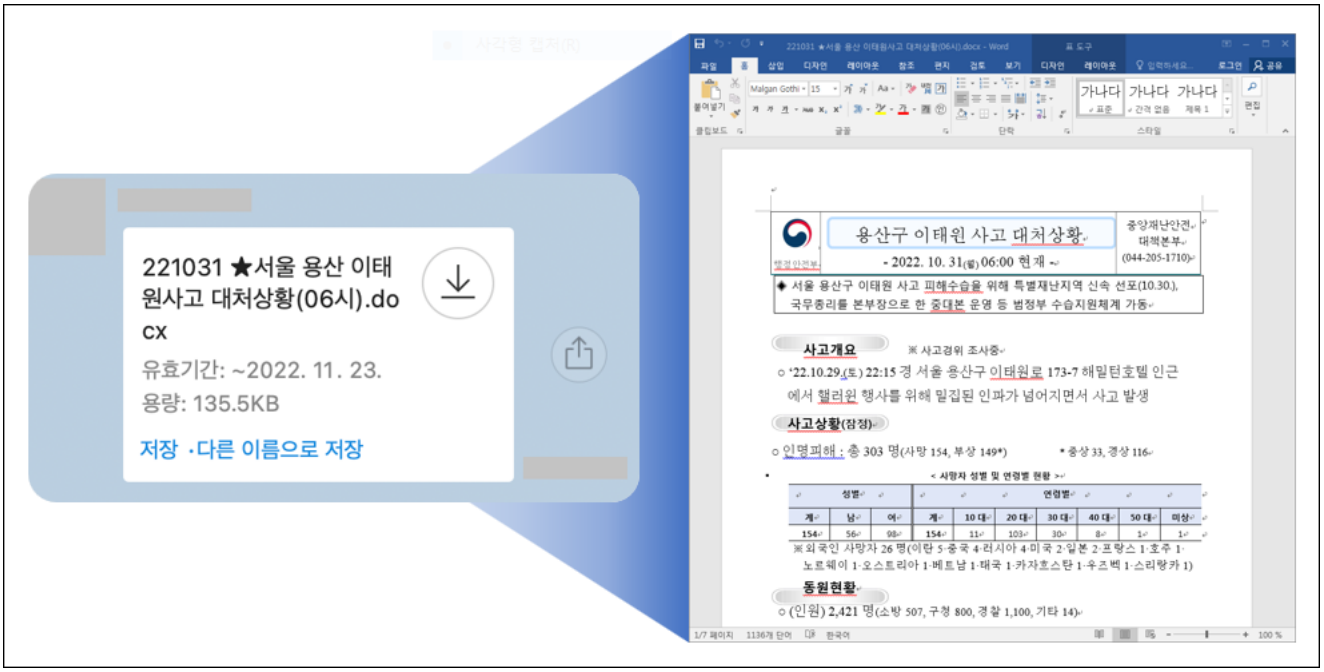
○ 특히, HWP, HWPX 문서 유형뿐만 아니라 LNK, DOCX, XLSX 파일을 활용한 공격도 동시다발적으로 수행하는 등 공격자는 이번 위협을 효과적으로 진행하기 위해 다양한 전술적 시도를 준비한 것으로 드러났습니다. 이 위협을 방어하기 위해 지니언스 고객은 Genian EDR을 사용해 APT37 활동을 감지하고, 단말 및 네트워크에 미치는 영향을 제한할 수 있습니다.

1.2. APT37 그룹의 취약점 활용 공격 사례

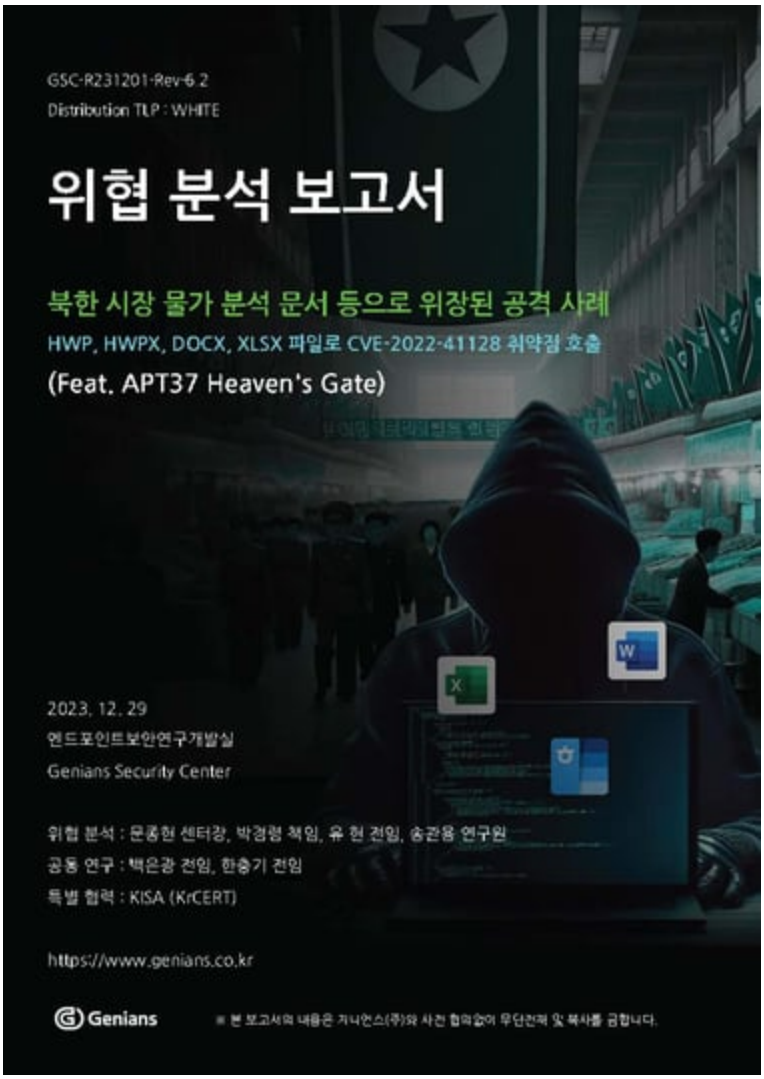
○ APT37 그룹은 과거에도 다양한 취약점을 활용해 공격을 수행했습니다. 대표적으로 인터넷 익스플로러(IE) Zero-Day 취약점이었던 'CVE-2022-41128' 사례가 있습니다. 2022년 10월 말, 북한분야 전문가들이 멤버로 가입된 특정 모바일 메신저 단체 대화방을 중심으로 다수의 DOCX 악성 문서가 한국에 유포된 바 있습니다.[3]

○ 이 사건은 한국에서 최초 식별된 이후 다양한 변종이 발견됐습니다. 특히, '용산 이태원 사고 대처상황'이라는 공문서를 사칭한 악성 DOCX 문서가 유포됐고, 일부 내용이 언론에 처음 기사화 됐습니다.[4] 이와 함께 한국인터넷진흥원 위협 인텔리전스 네트워크를 중심으로 민관 사이버 협력 채널이 즉시 가동돼 분석과 함께 C2 서버가 차단됐습니다. 그리고 대통령실 국가안보실에서 '이태원 사고 이슈 악용 사이버 위협 주의' 제목의 사이버안보비서관실 작성의 보도자료가 언론에 배포됐습니다.[5]

○ 그 당시 공격자는 이메일 기반 스피어 피싱 공격 전략도 구사했지만, DOCX 원격 템플릿 인젝션 기법으로 보안 취약점을 결합해 공격했습니다. 악성 파일을 유포할 때는 PC버전 모바일 메신저가 설치된 단말에 침투한 후, 피해자 계정에 몰래 접근해 특정 대화방 내 여러 사람들에게 악성 문서를 단계별로 유포했던 경우입니다.



[그림 1-1] 모바일 메신저로 유포된 'CVE-2022-41128' 공격 화면

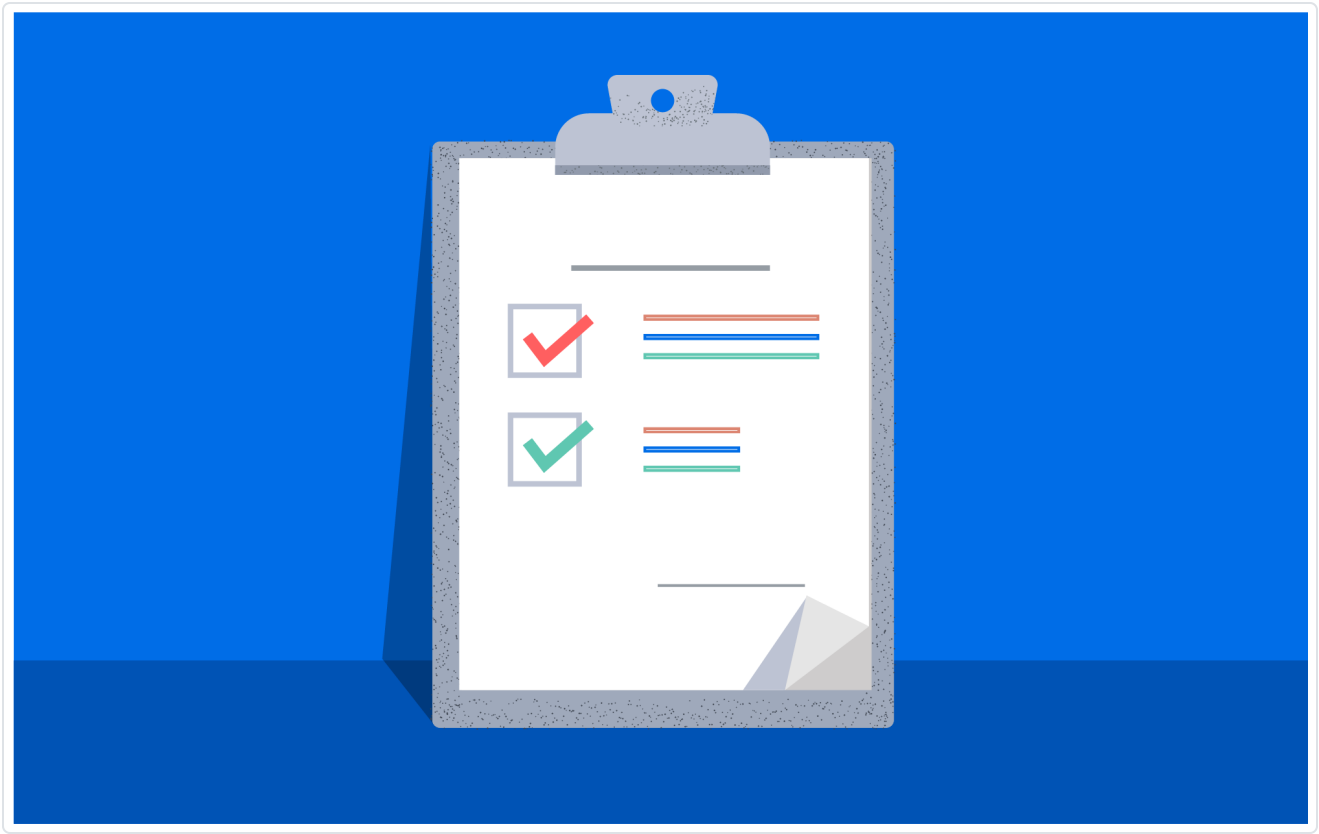


보고서 전문 보기

[1] HWP 문서 내부에 악성 OLE 삽입 공격 (FlowerPower APT 캠페인 Github C2 사용)
[2] HWPX 관련 자주하는 질문 및 답변안내
[3] Internet Explorer 0-day exploited by North Korean actor APT37
[4] [단독] '이태원 참사' 악용한 악성코드 공격 포착
[5] 안보실 "이태원 참사 보도자료로 위장한 악성문서 주의해야"

관련 컨텐츠

2024년 Webinar 안내장 사칭 APT 공격 포착



ATT&CK을 이용해 스스로 평가하기(APT3, Second Scenario)

북한 시장 물가 분석 문서 등으로 위장된 공격 사례

Happy Threat Hunting Part 2.

HWP 문서 내부에 악성 OLE 삽입 공격 FlowerPower APT 캠페인 Github C2 사용

지니언스 솔루션으로 매직라인 대응하기