No. 5

Report

암호화폐 기업 제휴 이슈로 가장한 북한 해킹 단체 코니(Konni) 추정 워드 문서 유포 분석 보고서

ZERO Co., Ltd.

2022 · 10 ANALYSIS REPORT

암호화폐 기업 제휴 이슈로 가장한 북한 해킹 단체 코니(Konni) 추정 워드 문서 유포 분석 보고서

암호화폐 기업 제휴 등 사회적 이슈의 제목으로 가장한 워드 문서 유포로
문서 파일 실행시 악성 매크로 실행을 유도하며, 매크로 실행시 IP정보(Ipv4,Ipv6) OS버전, 컴퓨터 이름의 정보가 C&C로 전송된다.

본 이슈는 '카뱅과 손잡은 코인원_비트 독주 체제 무너뜨릴까 [위클리 코인리뷰] - 이코노미스트' 파일명의 가지고 있으며 사회적 이슈 키워드를 사칭한 악성 문서 유포가 되겠다.

정상적인 기능을 악용해 악성 매크로를 사용하는 방식이며, 정상 소프트웨어를 통해 기능이 실행된다. 악성 매크로는 명령어를 통해 사용자가 실행할 경우 문서에 숨겨놓은 코드를 작동하도록 구성해두며, 사용자가 직접 '콘텐츠 사용' 버튼을 눌러야 악성 행위가 일어난다.

1. Non-PE 실행

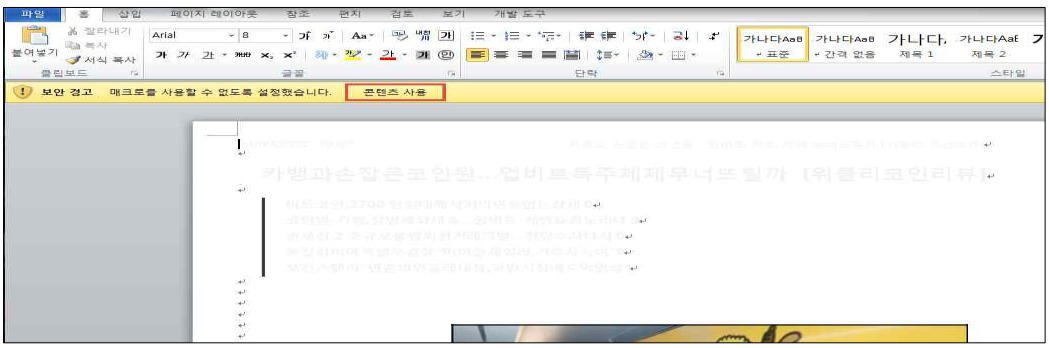

그림 1. 워드문서 실행 화면

파일을 실행하면 매크로를 사용하기위해 콘텐츠 사용을 유도 한다.

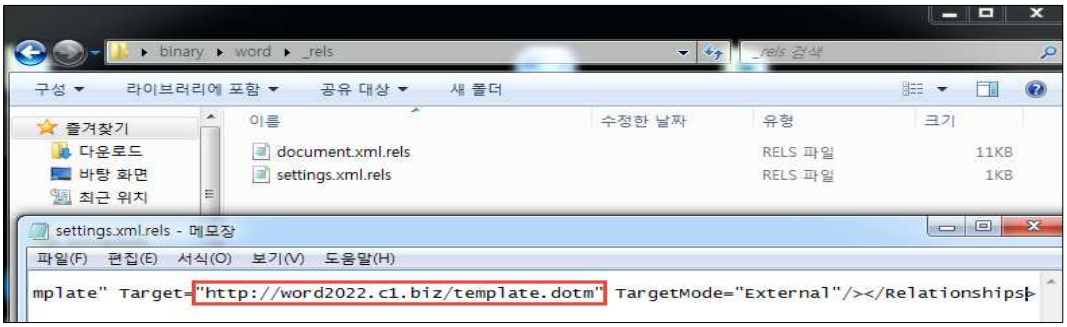

그림 2. Remote Template Injection

문서 파일 자체에는 매크로 기능이 들어 있지 않지만, hxxp://word2022[.]c1[.]biz/template.dotm URL에 접속하여 dotm 파일을 다운받아 매크로를 실행하게 된다. 취약점(CVE-2013-3906)을 이용하여 Remote Template Injection을 수행을 하는 것으로, 매크로 기능이 없는 문서를 이용하여 탐지를 우회하여 악성 매크로 기능이 있는 dotm 파일을 다운받아 매크로를 실행하게 된다.

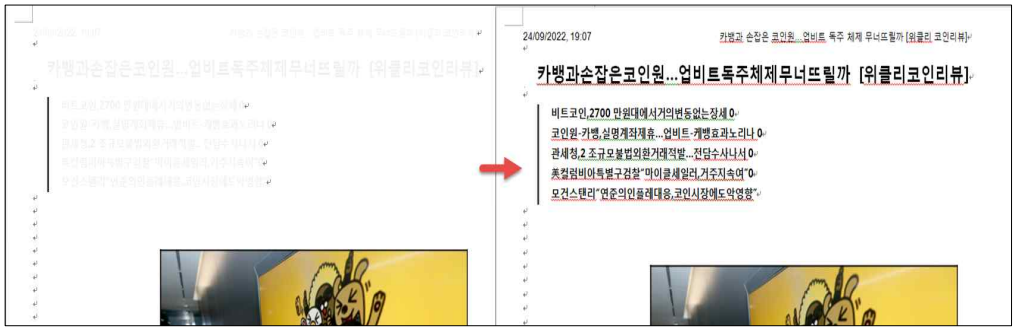

그림 3. docx 문서 매크로 실행 전/후

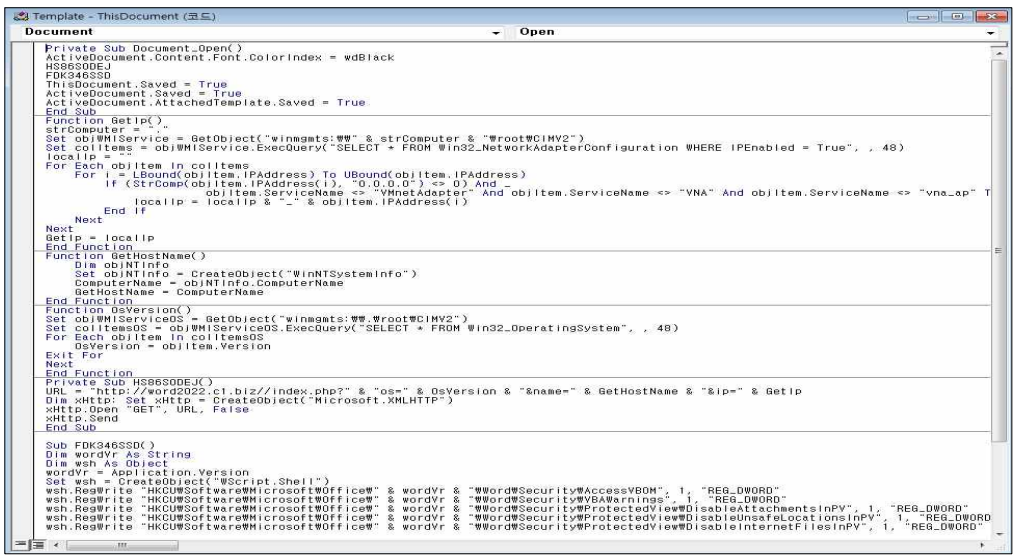

그림 4. docx 문서내 매크로 코드

다운받은 문서내 매크로 코드이며 아래의 설명과 같이 기기정보들을 수집한다.

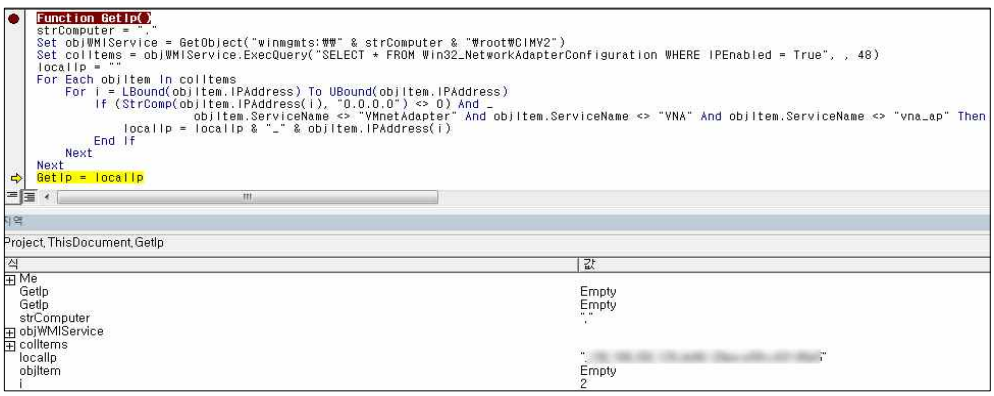

그림 5. IP 주소 수집

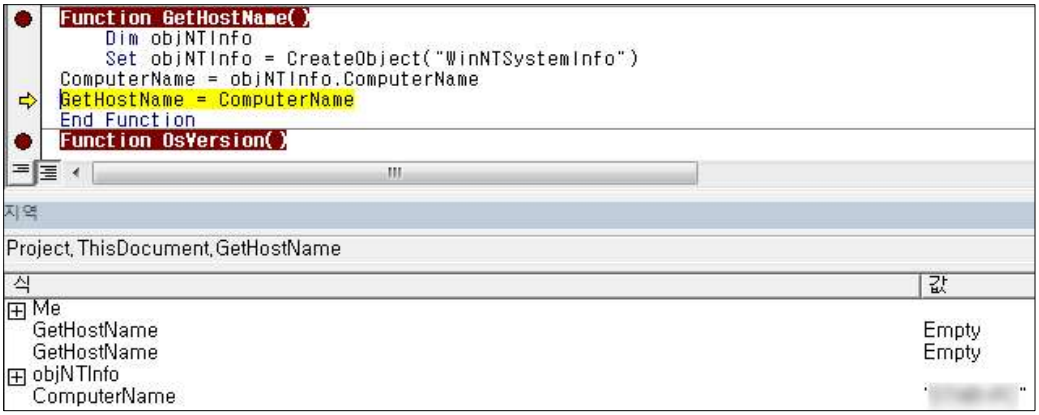

그림 6. PC 이름 수집

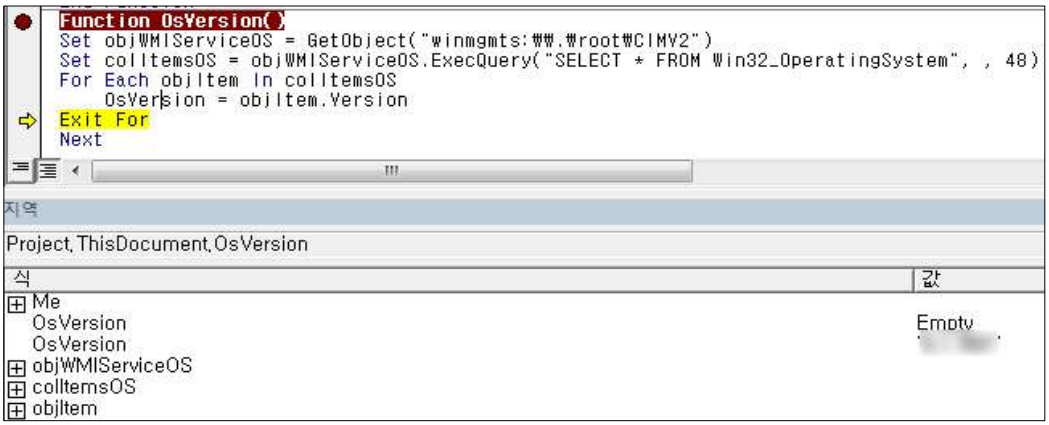

그림 7. OS 버전 수집

2. 네트워크

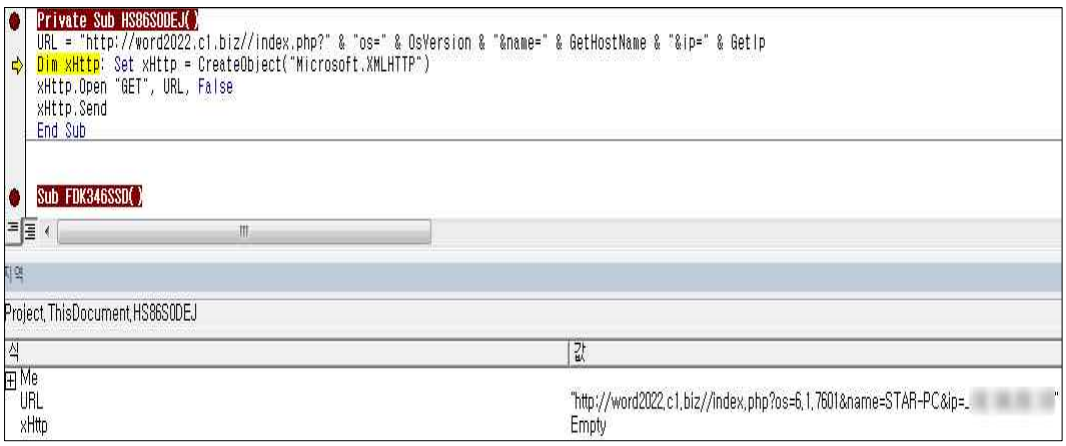

그림 8. 수집된 정보 유출

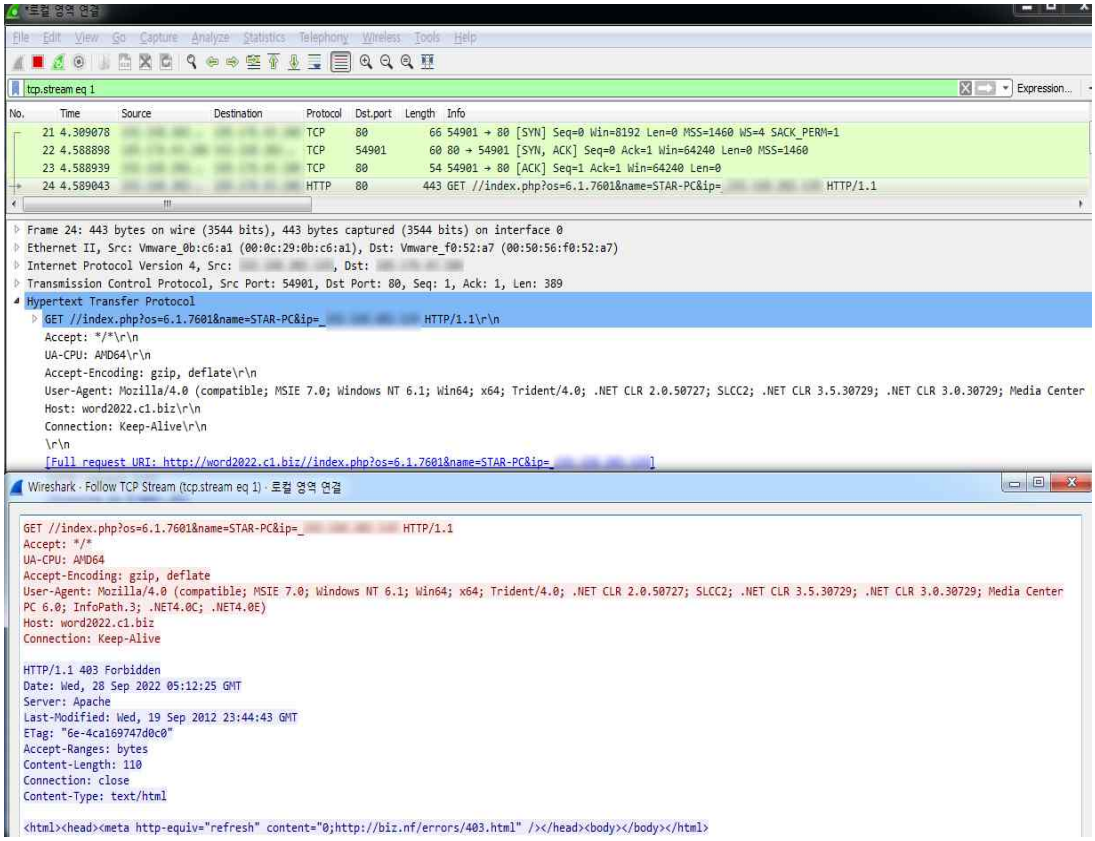

그림 9. C&C 서버 접속 정보

수집한 사용자의 기기정보(PC이름, IP, OS버전)을 C&C 서버로 전송한다.
C&C서버에서 수집한 정보를 기반으로 2차 악의적인 행위가 이뤄질 것으로 추정된다.

3. 결론

악성 매크로를 누르기 위해 궁금증을 유발해 사용자를 속이고 매크로를 실행하도록 유도하므로 출처가 불분명한 문서 파일의 콘텐츠 사용, 매크로 포함 버튼은 클릭하지 않아야 한다.

4. IoC 정보

md5 00e6e9ed4666623860686c123ed334f0 (docx)
md5 2C0DB5D995D997A7687F527C493B4C89 (dotm)
hxxp://word2022.c1.biz/template.dotm
hxxp://word2022.c1.biz/index.php

* 추가 관련정보는 사이버위협 대응 포털 플랫폼 ZeroBOX 에서 확인하실 수 있습니다.