Posted on May 3, 2022

Distribution of Malicious Word File Related to North Korea's April 25th Military Parade

On April 29th, the ASEC analysis team discovered the distribution of a malicious Word file related to North Korea's military parade. The distributor uploaded the file on a Korean web server which is assumed to have been breached. Besides the malicious Word file, the server also had 2 normal HWP files, likely used for distributing malicious HWP files with the OLE object or EPS vulnerability method.

— [Analysis] North Korea's Position on Use of Nuclear Weapons and Implications of Changes in Military Elites Based on April 25th Military Parade.docm (malicious: inside data.zip) — "Channel A news anchor Ha Jong-dae joins Yoon Suk-yeol's election camp".hwp (normal) — attach.hwp (normal)

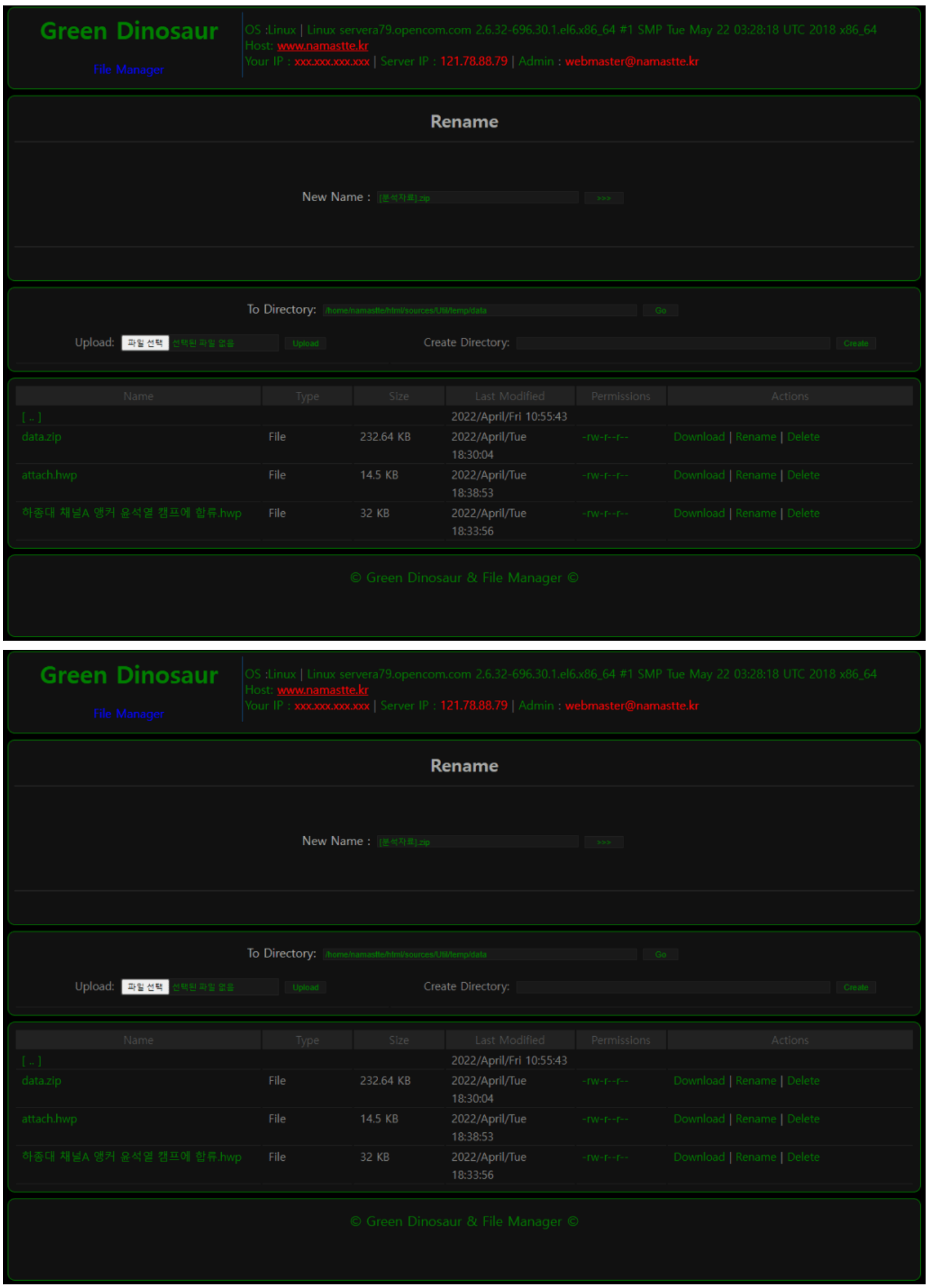
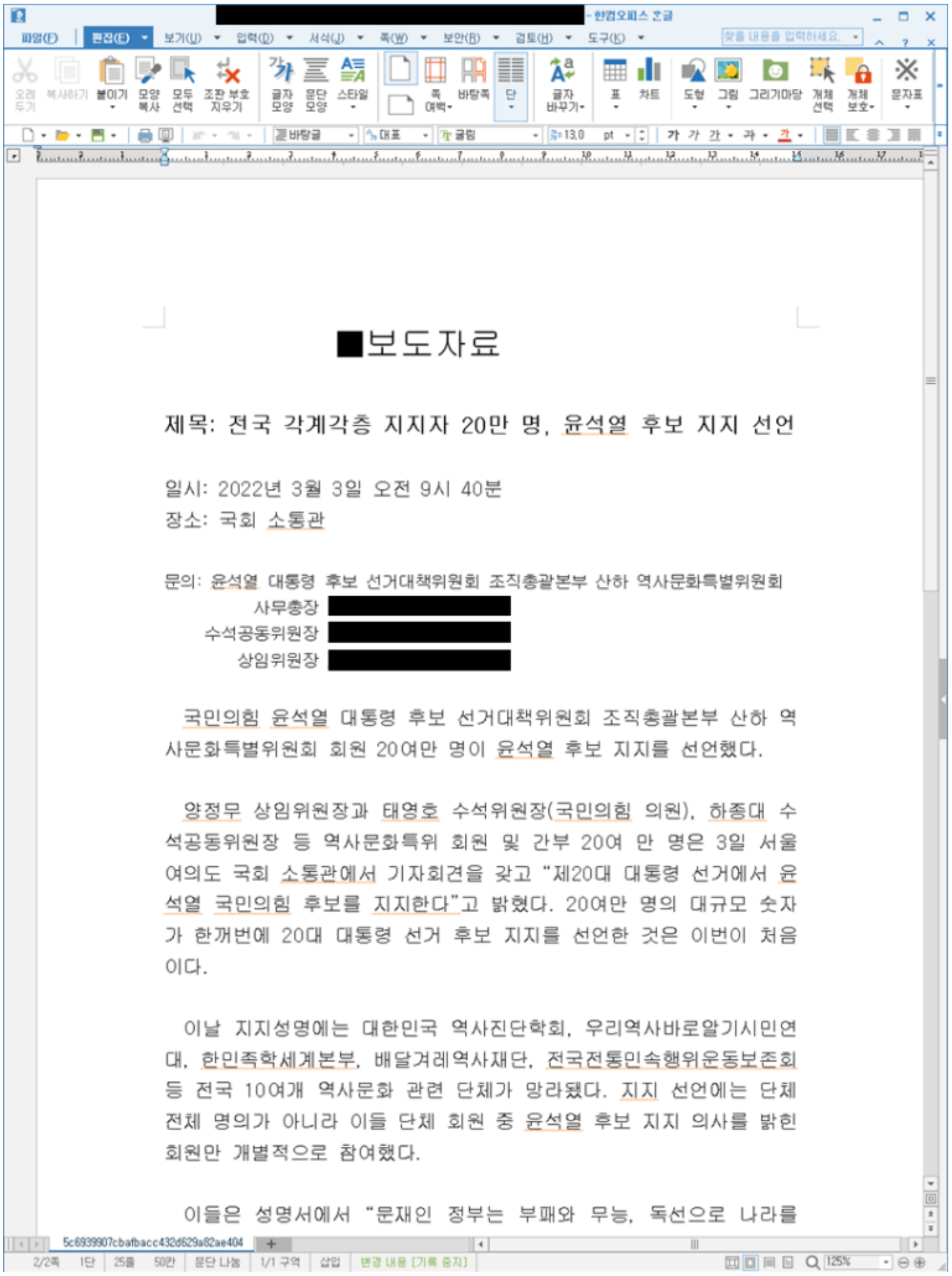


Figure 1. Server webpage uploaded with malicious Word file (data.zip)


[redacted] - 한컴오피스 한글
파일(F) 편집(E) 보기(V) 입력(D) 서식(J) 쪽(W) 보안(B) 검토(H) 도구(K)
찾을 내용을 입력하세요.
■보도자료
제목: 전국 각계각층 지지자 20만 명, 윤석열 후보 지지 선언
일시: 2022년 3월 3일 오전 9시 40분
장소: 국회 소통관
문의: 윤석열 대통령 후보 선거대책위원회 조직총괄본부 산하 역사문화특별위원회
사무총장 [redacted]
수석공동위원장 [redacted]
상임위원장 [redacted]
국민의힘 윤석열 대통령 후보 선거대책위원회 조직총괄본부 산하 역사문화특별위원회 회원 20여만 명이 윤석열 후보 지지를 선언했다.
양정무 상임위원장과 태영호 수석위원장(국민의힘 의원), 하종대 수석공동위원장 등 역사문화특위 회원 및 간부 20여 만 명은 3일 서울 여의도 국회 소통관에서 기자회견을 갖고 "제20대 대통령 선거에서 윤석열 국민의힘 후보를 지지한다"고 밝혔다. 20여만 명의 대규모 숫자가 한꺼번에 20대 대통령 선거 후보 지지를 선언한 것은 이번이 처음이다.
이날 지지성명에는 대한민국 역사진단학회, 우리역사바로알기시민연대, 한민족학세계본부, 배달겨레역사재단, 전국전통민속행위운동보존회 등 전국 10여개 역사문화 관련 단체가 망라됐다. 지지 선언에는 단체 전체 명의가 아니라 이들 단체 회원 중 윤석열 후보 지지 의사를 밝힌 회원만 개별적으로 참여했다.
이들은 성명서에서 "문재인 정부는 부패와 무능, 독선으로 나라를

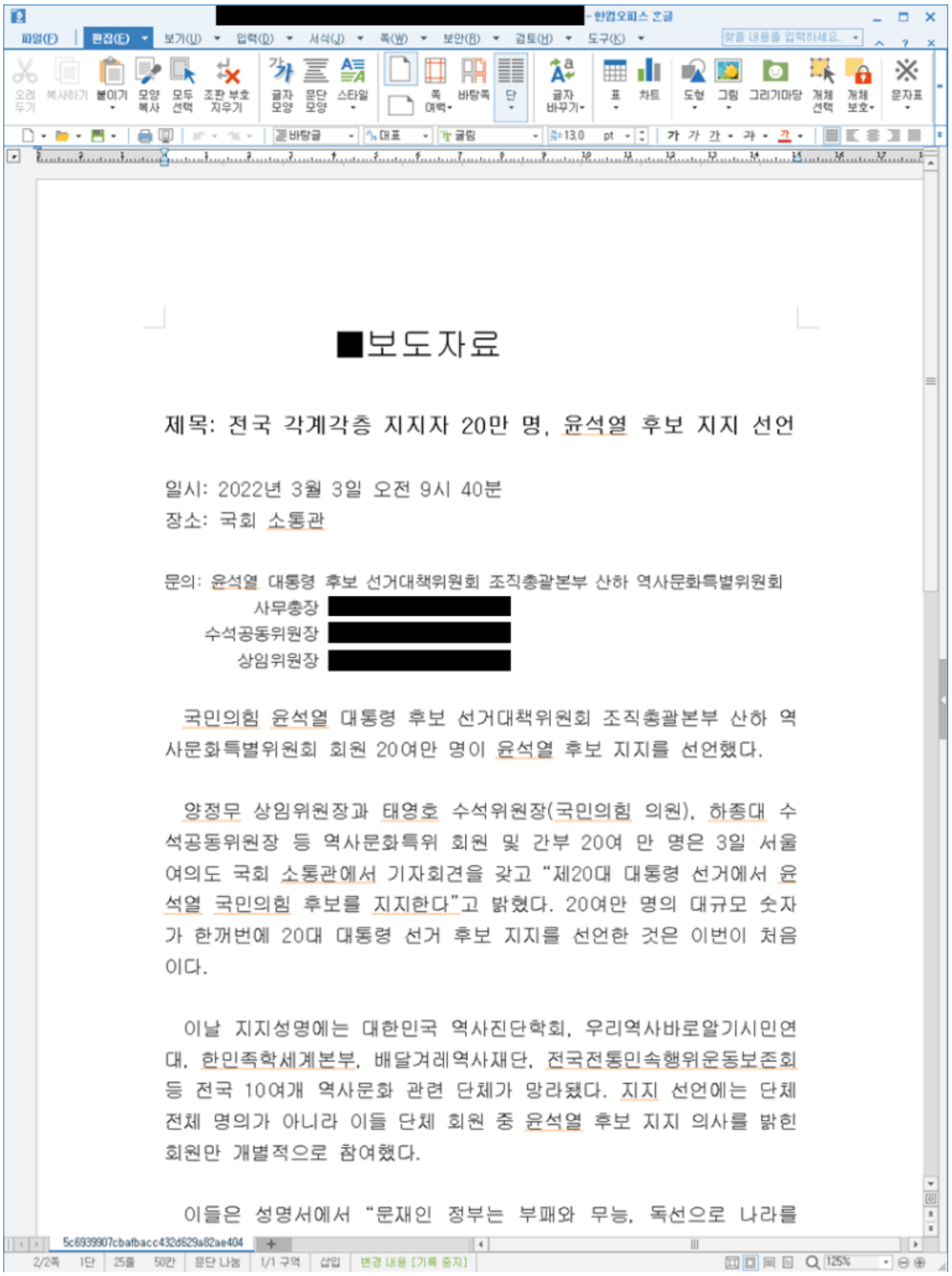
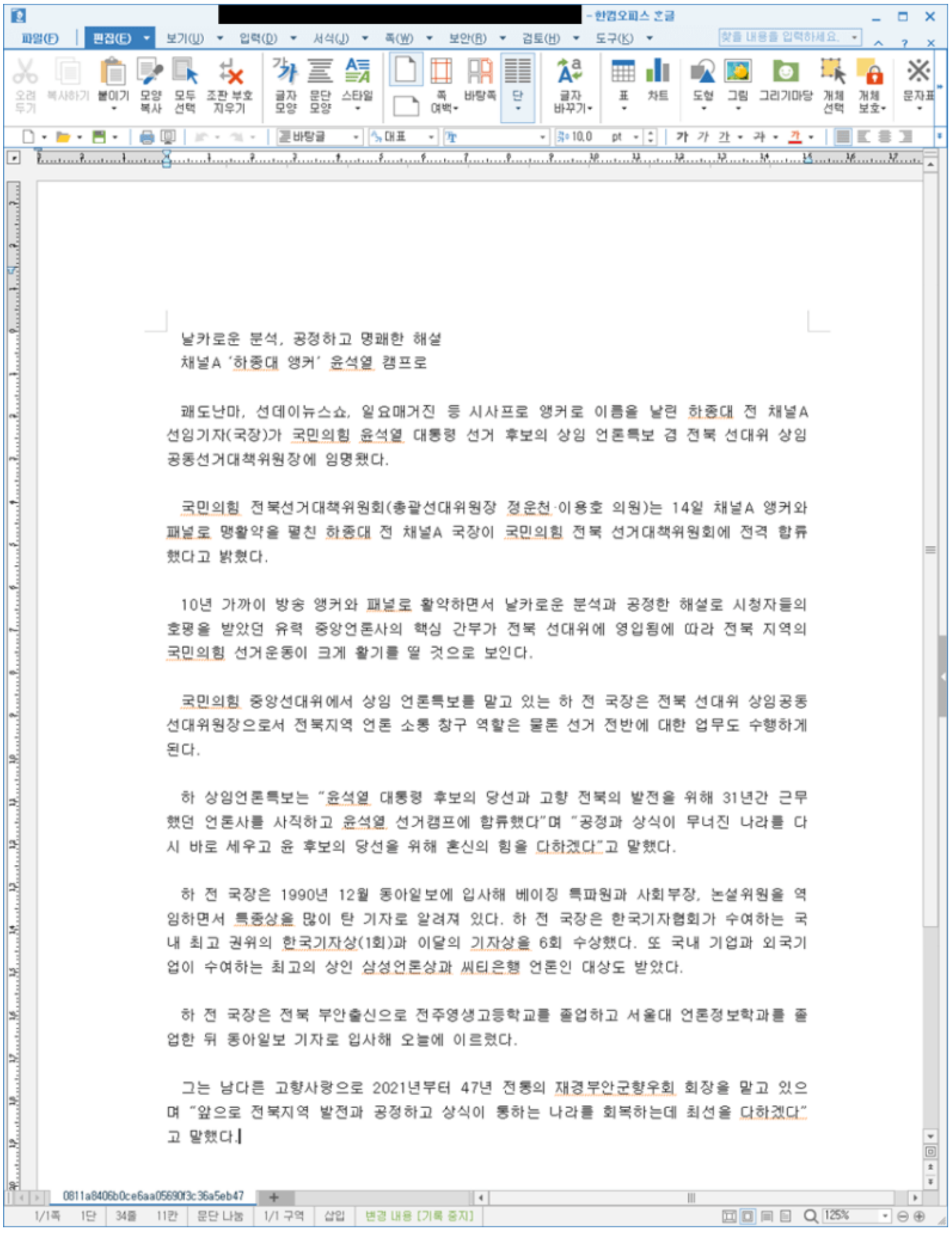


Figure 2. attach.hwp (created on: March 2nd, 2022 Wednesday 3:36:27 P.M.)


[redacted] - 한컴오피스 한글
파일(F) 편집(E) 보기(V) 입력(D) 서식(J) 쪽(W) 보안(B) 검토(H) 도구(K)
찾을 내용을 입력하세요.
오려 두기 복사하기 붙이기 모양 복사 모두 선택 조판 부호 지우기
글자 모양 문단 모양 스타일 쪽 여백 바탕쪽 단
글자 바꾸기 표 차트 도형 그림 그리기마당 개체 선택 개체 보호 문자표
바탕글 대표 10.0 pt
날카로운 분석, 공정하고 명쾌한 해설
채널A '하종대 앵커' 윤석열 캠프로
쾌도난마, 선데이뉴스쇼, 일요매거진 등 시사프로 앵커로 이름을 날린 하종대 전 채널A 선임기자(국장)가 국민의힘 윤석열 대통령 선거 후보의 상임 언론특보 겸 전북 선대위 상임 공동선거대책위원장에 임명됐다.
국민의힘 전북선거대책위원회(송관선대위원장 정운천·이용호 의원)는 14일 채널A 앵커와 패널로 맹활약을 펼친 하종대 전 채널A 국장이 국민의힘 전북 선거대책위원회에 전격 합류했다고 밝혔다.
10년 가까이 방송 앵커와 패널로 활약하면서 날카로운 분석과 공정한 해설로 시청자들의 호평을 받았던 유력 중앙언론사의 핵심 간부가 전북 선대위에 영입됨에 따라 전북 지역의 국민의힘 선거운동이 크게 활기를 띨 것으로 보인다.
국민의힘 중앙선대위에서 상임 언론특보를 맡고 있는 하 전 국장은 전북 선대위 상임공동선대위원장으로서 전북지역 언론 소통 창구 역할은 물론 선거 전반에 대한 업무도 수행하게 된다.
하 상임언론특보는 "윤석열 대통령 후보의 당선과 고향 전북의 발전을 위해 31년간 근무했던 언론사를 사직하고 윤석열 선거캠프에 합류했다"며 "공정과 상식이 무너진 나라를 다시 바로 세우고 윤 후보의 당선을 위해 혼신의 힘을 다하겠다"고 말했다.
하 전 국장은 1990년 12월 동아일보에 입사해 베이징 특파원과 사회부장, 논설위원을 역임하면서 특종상을 많이 탄 기자로 알려져 있다. 하 전 국장은 한국기자협회가 수여하는 국내 최고 권위의 한국기자상(1회)과 이달의 기자상을 6회 수상했다. 또 국내 기업과 외국기업이 수여하는 최고의 상인 삼성언론상과 씨티은행 언론인 대상도 받았다.
하 전 국장은 전북 부안출신으로 전주영생고등학교를 졸업하고 서울대 언론정보학과를 졸업한 뒤 동아일보 기자로 입사해 오늘에 이르렀다.
그는 남다른 고향사랑으로 2021년부터 47년 전통의 재경부안군향우회 회장을 맡고 있으며 "앞으로 전북지역 발전과 공정하고 상식이 통하는 나라를 회복하는데 최선을 다하겠다"고 말했다.
0811a8406b0ce6aa05690f3c36a5eb47
1/1쪽 1단 34줄 11칸 문단 나눔 1/1 구역 삽입 변경 내용 [기록 중지] 125%

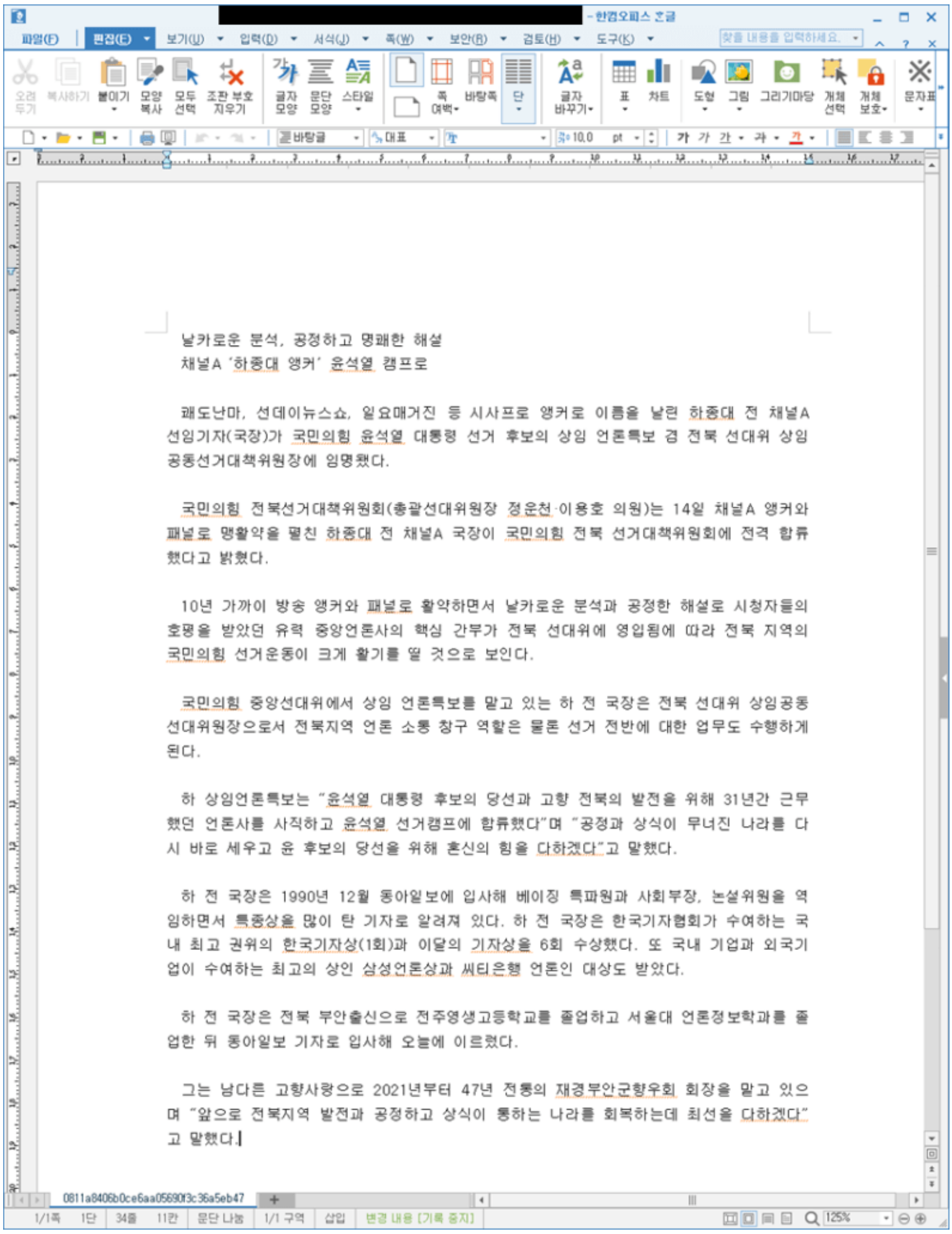


Figure 3. "Channel A news anchor Ha Jong-dae joins Yoon Suk-yeol's election camp".hwp (created on: February 25th, 2022 Friday 12:38:15 A.M.)

While the team could not secure the file as "data.zip" uploaded on the attacker's server was encrypted, it is likely that the attacker used wscript.exe like in previous attacks to perform malicious behaviors such as leaking the PC information.

The attacker is continuously attacking personnel in the field of national defense, politics, and diplomacy. Since malicious Word files are mainly distributed in the form of e-mail attachments, users should refrain from opening attachments of e-mails received from unknown sources and enabling macros.

AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below.

[File Detection] Trojan/HTML.Loader(2022.04.30.00)

[IOC] 6cc09bc6e605b59d7eb48eb266f798f8 (HTML) hxxp://www.namastte[.]kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/data&rename=[Analysis].zip (HTML)

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

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

Categories:Malware Information