악성문서 분석 가이드라인

[중간 발표]

송태현 김현진 허송이 이다영

목차

① 자료 수집 :: 악성 문서 샘플 수집

파일 정보

- 파일 타입: 한글 워드프로세서 문서
- 파일명: kinu 전문가 자문 요청사항(한미동맹과 한중관계).hwp (추정)
- MD5: 42ae424f27d83fa132b2967b64f6ba21

① 자료 수집 :: 가이드라인 조사

7. kinu 전문가 자문 요청사항(한미 동맹과 한중관계) [virus total : 22]

- https://sfkino.tistory.com/75
- https://jeongzzang.com/129
- https://asec.ahnlab.com/1253
- https://support.ahnlab.com/hc/ko/articles/360047808354-Kimsuky-%EC%A1%B0%EC%A7%81-%EC%95%85%EC%84%B1-HWP-%ED%95%9C%EA%B8%80-%EB%AC%B8%EC%84%9C-%EC%9C%A0%ED%8F%AC >> 안랩 블로그
- https://asec.ahnlab.com/1265 >> 안랩 블로그

8. 미국 라스베가스 CES 2020 참관단 [virus total : 31]

- https://asec.ahnlab.com/1256 >> 안랩 블로그
- https://blog.alyac.co.kr/2581

② 악성 문서 분석 :: 삽질

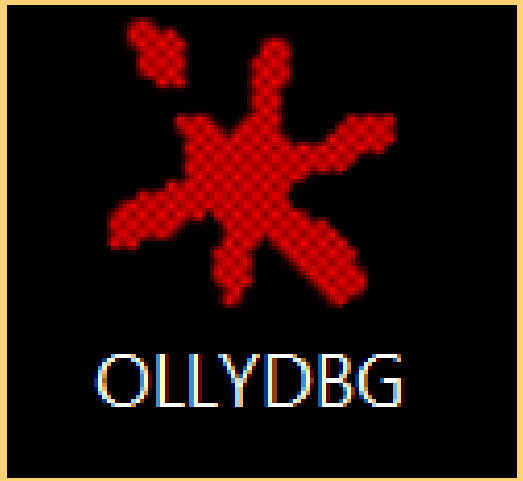
Scan Result

Name	Vulnerability	Scan Engine
DocInfo	OK	
PrvText	OK	
DefaultJScript	OK	
JScriptVersion	OK	
Section1	Exploit.HWP.Generic.43	hwptag.nhp
Section2	Exploit.HWP.Generic.43	hwptag.nhp
Section3	Exploit.HWP.Generic.43	hwptag.nhp
Section4	Exploit.HWP.Generic.43	hwptag.nhp
Section5	Exploit.HWP.Generic.43	hwptag.nhp
Section0	OK	
PrvImage	OK	
_LinkDoc	OK	
FileHeader	OK	
|HwpSummaryInformation	OK	

000001D4	0016	HWPTAG_PARA_HEADER	문단 헤더
000001EE	100035A	HWPTAG_PARA_TEXT	문단의 텍스트
01000550	0008	HWPTAG_PARA_CHAR_SHAPE	문단의 글자 모양

② 악성 문서 분석 :: 삽질

```
01000130  0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 90  ................
01000140  57 56 52 53 55 51 33 c9 ba 0c 0c 0c 0c 42 3e 8a  WVRSUQ3......B>.
01000150  02 3c 0c 74 f8 8b da 83 c2 2a 3e 80 32 fa 42 41  .<.t.....*>.2.BA
01000160  81 f9 e4 03 00 00 72 f2 90 90 af 71 16 7b 16 66  ......r....q.{.f
01000170  fa fa fa a9 ac ad 3d bf 06 fa fa fa fa 3d bf 02  ......=......=..
01000180  fa fa fa fa 73 67 96 05 05 05 11 94 06 c9 3a 9e  ....sg........:.
01000190  71 ba ca c4 71 ba f6 c4 71 8a e6 57 c4 71 92 f2  q...q...q..W.q..
```



② 악성 문서 분석 :: 포렌식

KINU 전문가 자문 요청사항

■ 자문 개요

o 본 연구는 2019년 통일연구원 일반협동과제(제목: 「2030년 미중관계와 한국의 대북·통일전략」)의 일부로서, 세부 자문주제는 "**최근 미중 전략적 경쟁과 갈등이 심화되고 있는 상황에서, 한국의 입장에서 미중관계를 어떻게 '활용'해야 하는지, 그리고 '새로운 한반도'를 위한 바람직한 한미동맹(or 한중관계)의 방향은 무엇인가에 대한 정책방안을 마련**"하고자 하는 것입니다.

■ 세부 자문 내용(아래 질문(Q1~3) 중심으로 논의할 예정입니다.)

② 악성 문서 분석 :: 포렌식

[그림]

EPS

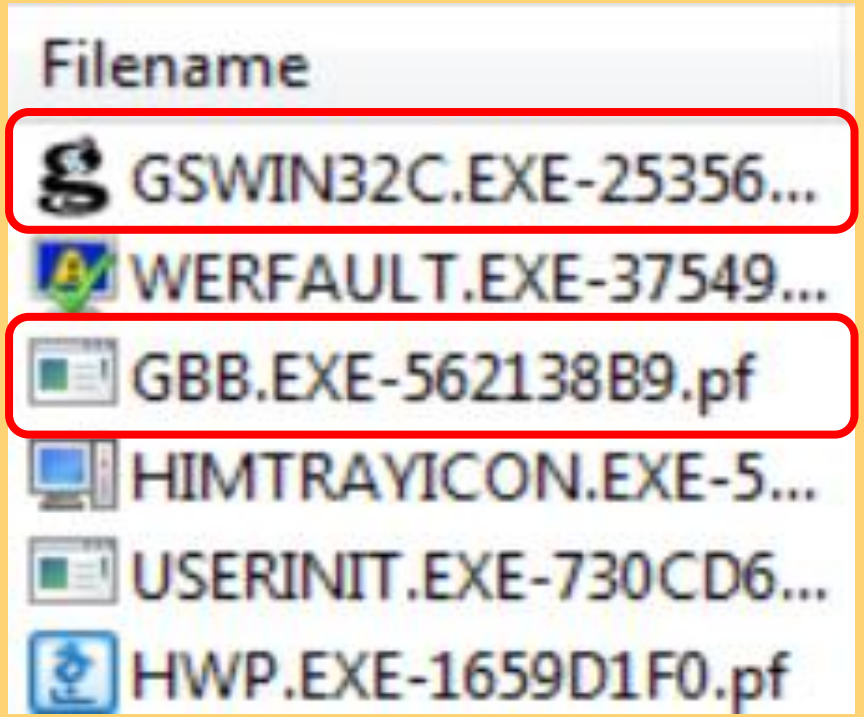
KINU 전문가 자문 요청사항

■ 자문 개요

○ 본 연구는 2019년 통일연구원 일반협동과제(제목: 「2030년 미중관계와 한국의 대북·통일전략」)의 일부로서, 세부 자문주제는 **"최근 미중 전략적 경쟁과 갈등이 심화되고 있는 상황에서, 한국의 입장에서 미중관계를 어떻게 '활용'해야 하는지, 그리고 '새로운 한반도'를 위한 바람직한 한미동맹(or 한중관계)의 방향은 무엇인가에 대한 정책방안을 마련"**하고자 하는 것입니다.

■ 세부 자문 내용(아래 질문(Q1~3) 중심으로 논의할 예정입니다.)

② 악성 문서 분석 :: 포렌식



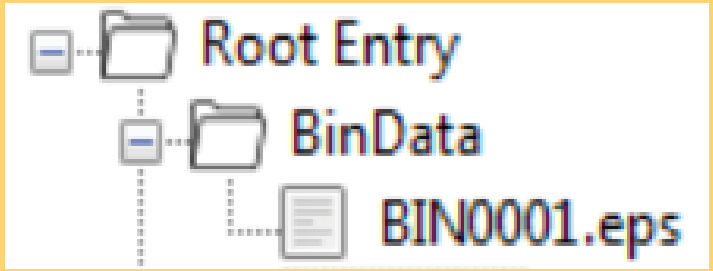
악성 한글문서 실행 이후 함께 실행된 파일

② 악성 문서 분석 :: 포렌식

GBB.EXE

▶ 포스트스크립트를 불러오는 프로세스 (gsdll32.dll 로드해서 동작)

▶ EPS 파일을 실행시킴



별도의 인터프리터 필요

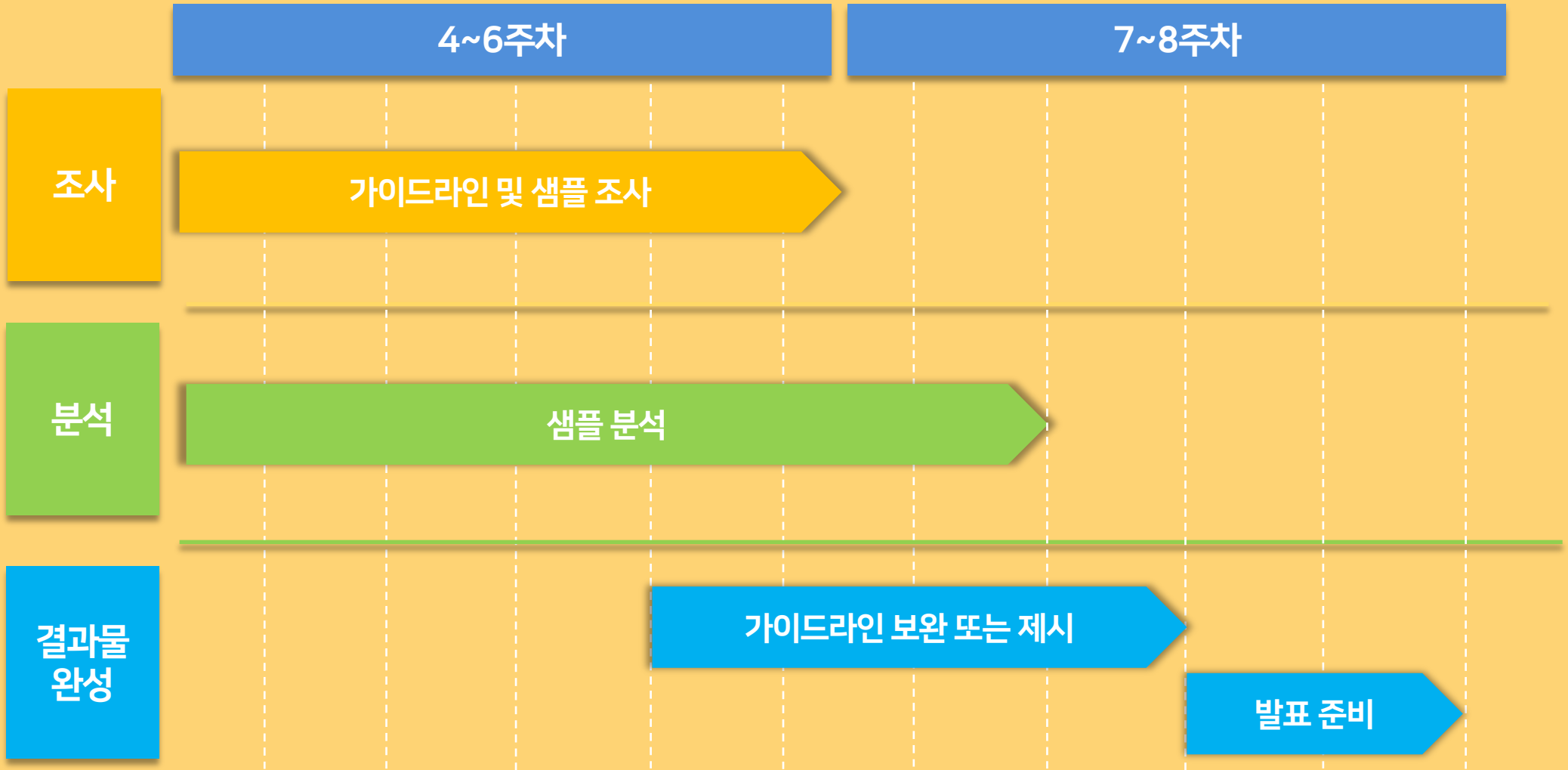
② 악성 문서 분석 :: 포렌식

GSWIN32C.EXE

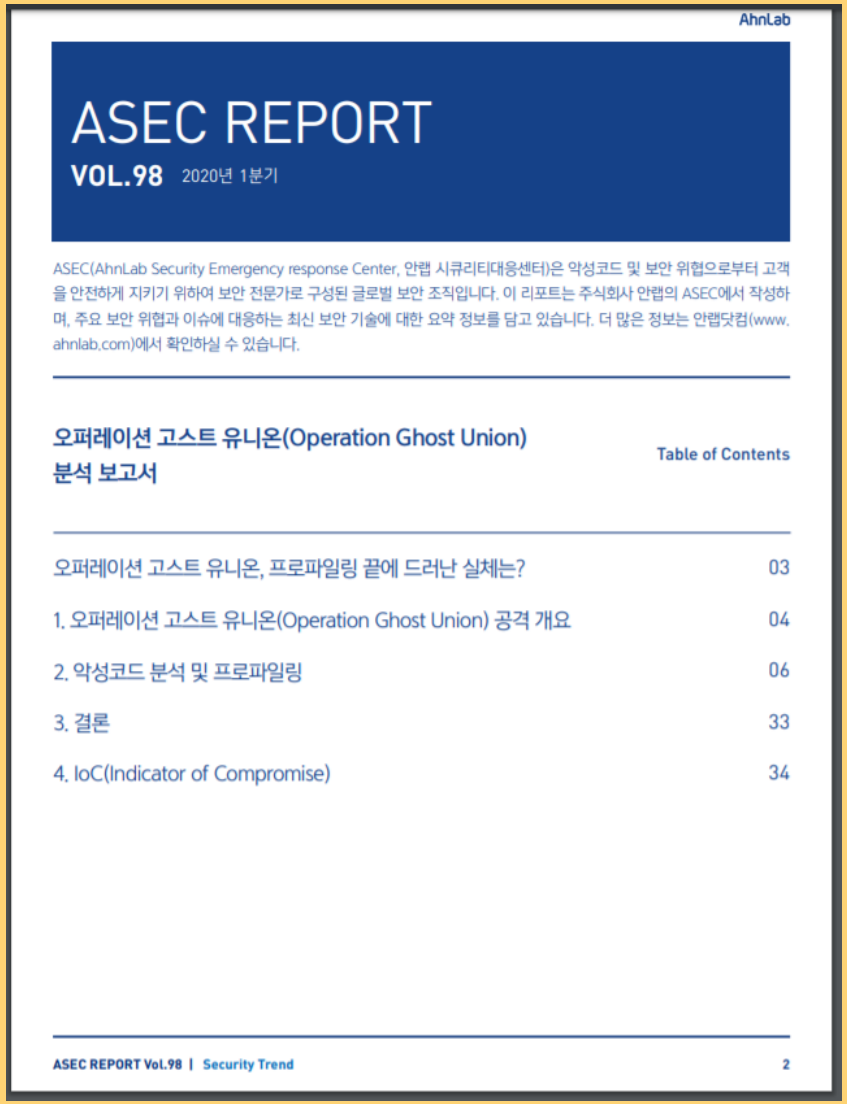
▶ tmp 파일을 실행시킴

▶tmp 파일을 열어본 결과, tmp 파일은 eps 파일을 tmp 파일에 덮어씌운 뒤, 최종적으로 eps 를 실행시킴

③ 차후 계획



③ 차후 계획:: 가이드라인 문서화 작성



AhnLab

ASEC REPORT

VOL.98 2020년 1분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

오퍼레이션 고스트 유니온(Operation Ghost Union) 분석 보고서

Table of Contents

가이드 라인 내용

1.악성문서 명

2. 사용된 실행파일

3. 악성문서 분석 내용

4. 진단 과정

Q & A

감사합니다 ☺