‘2021년 국방부 업무보고 수정’ 문서로 위장한 악성코드 유포

asec.ahnlab.com/ko/20057/

2021년 2월 3일

1월 24일 ASEC에서는 ‘2021년 국방부 업무보고 수정’문서로 위장하여 악성코드가 함께 유포된 정황을 확인하였다. 해당 악성코드의 확장자는 아래와 같이 *.pif로 만들어져 유포되었으며 이는 EXE 확장자와 같은 실행 가능한 파일이다. 파일 실행 시 아래의 그림과 같이 현재 국방부 홈페이지에서 제공하는 정상 PDF 문서의 내용과 동일한 파일이 사용자에게 보여진다. 하지만, 정상 PDF 문서파일과 함께 (사용자 모르게) 악성 파일(DLL형식)이 생성 및 실행되는 구조를 갖는다.

유포 파일 명

2021년 국방부 업무보고 수정.pif

생성 파일

- %원본파일 경로%\2021년 국방부 업무보고 수정.pdf (정상문서)
- C:\ProgramData\Intel\Driver\driver.cfg (악성 DLL 파일)

2021년 국방부 업무보고

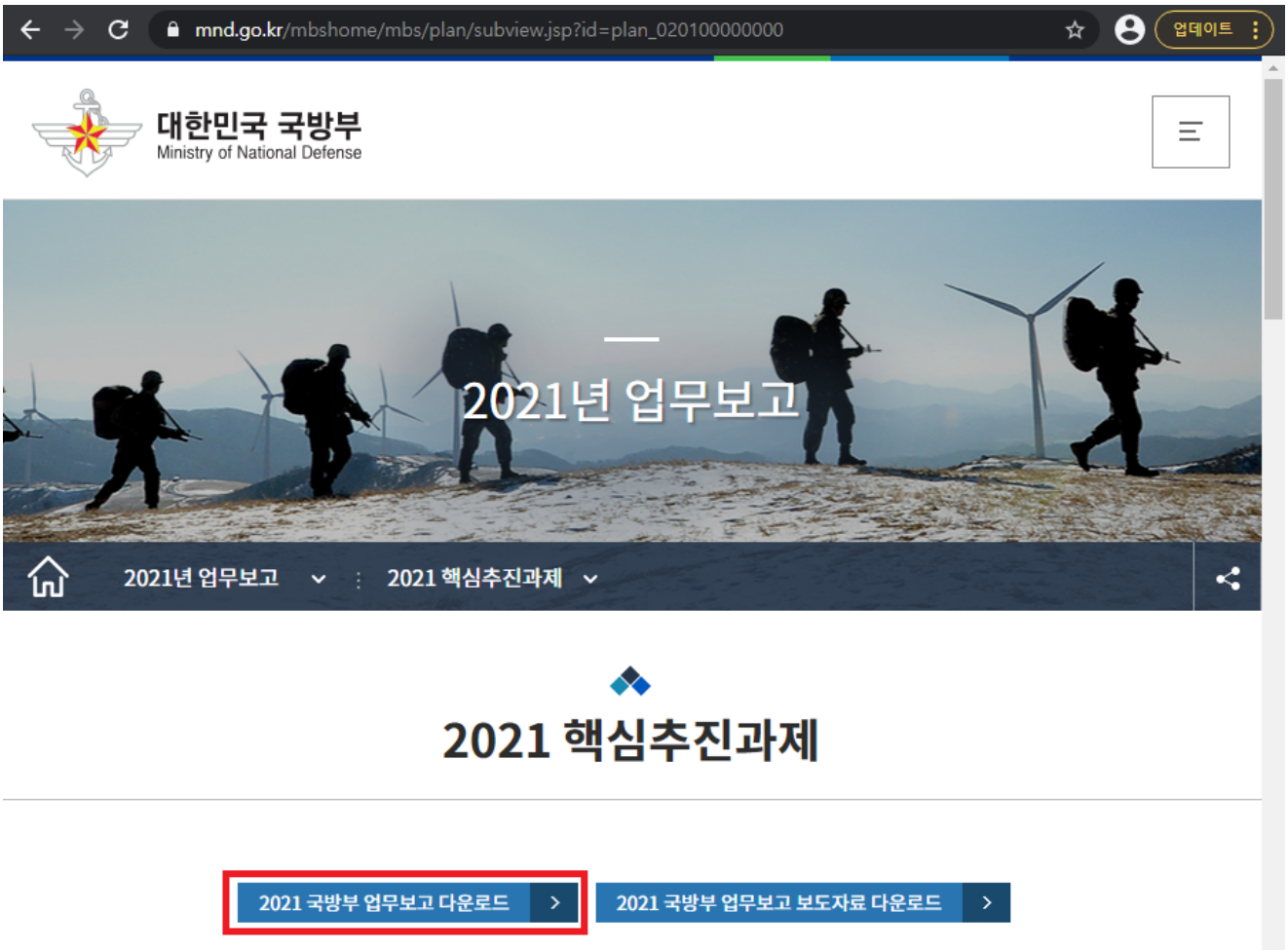
2021. 1. 21. (목)

"강한 안보, 자랑스러운 군, 함께하는 국방"

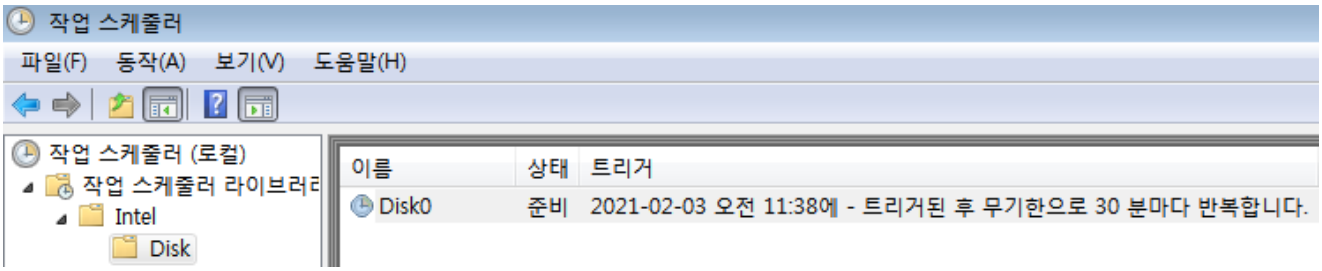
국 방 부

생성된

정상 ‘2021년 국방부 업무보고 수정.pdf’



실제 국방부 홈페이지에 업로드 된 문서와 같은 내용으로 유포
생성된 악성 DLL 파일은 regsvr32.exe를 통해 실행되며 아래 그림과 같이 'Disk0'이라는 명으로 스케줄 등록되어 30분마다 실행된다.



30분 단위로 실행될 수 있도록 스케줄 등록

PE Header

Item	Values	Comment
Machine	8664	
Number of Sections	3	
TimeStamp	600b852d	Jan 23 2021 11:08:45 GMT+09
Pointer to Symbol Table	00000000	
Number of Symbols	00000000	0
Size of Optional Header	000000f0	240
Characteristics	2022	DLL
Magic	020b	
Major/Minor Linker Version	14. 26	
Size of Code	00017000	94,208
Size of Initialized Data	00001000	4,096
Address of Entry Point	00043860	276,576
First Bytes	48894c24	
Base of Code	0002d000	184,320
Base of Data	00000000	0
Image Base	0000000180000000	
Section Alignment	00001000	
File Alignment	00000200	

2021년 1월 23일 컴파일 된 악성 DLL
최종적으로 C2접속 후 공격자로부터 명령을 받아 추가 악성 행위가 수행될 것으로 보인다.

현재 해당 악성 파일은 아래와 같이 V3에서 진단 중이다.

[파일 진단]

- Downloader/Win64.Agent.C4318031
- Trojan/Win64.Agent.C4318029

[관련 IoC]

- hxxp://exchange.amikbvx.cf/
- hxxp://imap.pamik.cf/
- 7e041b101e1e574fb81f3f0cdf1c72b8
- 447163d776b62bf0b1c652c996cc0586

Categories:악성코드 정보