No. 1

Report

엑셀 문서를 통해 유포중인 Emotet 악성코드

ZERO Co., Ltd.

2022 · 08 ANALYSIS REPORT

엑셀 문서를 통해 유포되는 Emotet 악성코드 분석 보고서

Emotet 악성코드는 MS 엑셀 파일을 이용하여 숨김시트와 매크로 실행을 유도, DLL 실행파일을 통한 PC 정보(컴퓨터이름, 볼륨시리얼넘버, 실행중인 프로세스 목록) 수집후 특정 C&C IP로 정보 유출.
다수의 DLL 유포지 URL, C&C를 이용하는 특징을 가지고 있음

최근 Emotet 악성코드를 다운로드하는 악성 엑셀 문서가 이메일을 통해 활발히 유포중에 있다. 업무 메일을 가장한 제목으로 꾸준히 유포중에 있으며 엑셀 파일의 매크로 실행을 유도하며 탐지 및 분석시스템 회피 목적의 압축 파일에 비밀번호를 걸어 유포하기도 한다.

1. Non-PE 실행

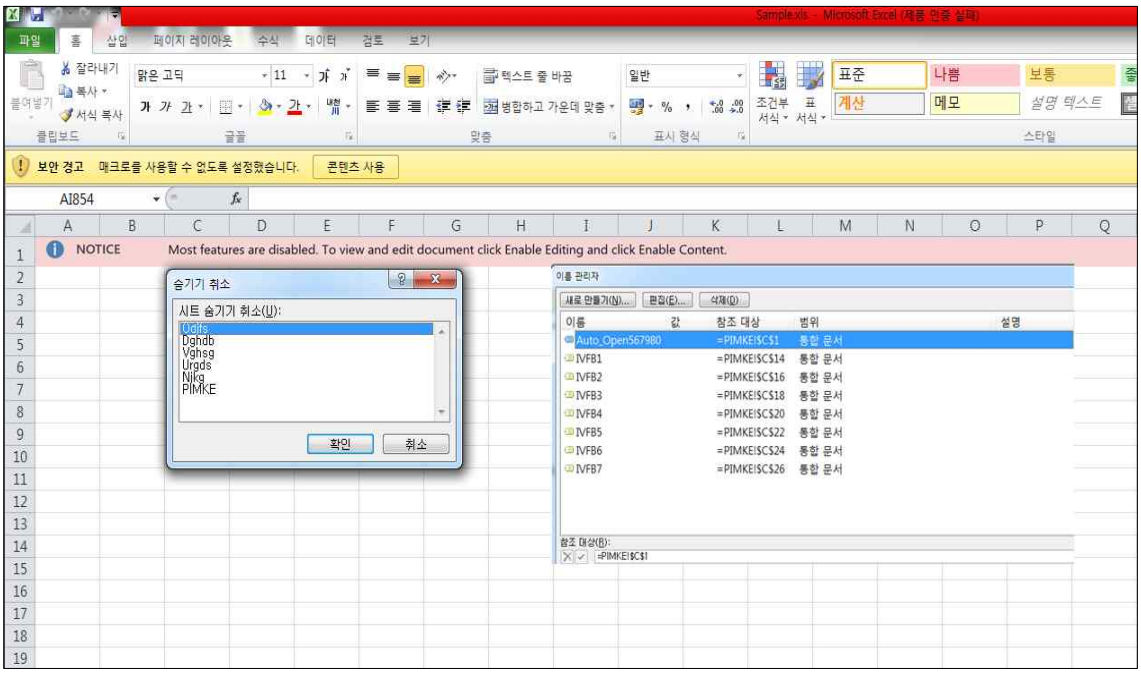

그림 1. 매크로 사용 및 숨김시트 액셀파일

매크로 시트는 Auto_Open 등으로 이름이 지정되거나 없을 경우 A1셀의 수식을 첫 번째로 실행한다.
이후 현재 실행중인 열(Column) 아래 방향으로 코드 흐름이 진행된다. =EXEC()은 개별 프로그램을 실행하는 함수이며, =RETURN으로 현재 실행 중인 함수만 중단을 하며 종료한다.

그림 2. 다수의 DLL 유포지 및 실행 매크로

숨김시트와 매크로를 통해 추가로 생성되는 수식은 특정 DLL 유포지 주소로부터 다운로드 하며, 다운이 안 될 경우, 순차적으로 다음 DLL 유포지 다운로드를 진행후 xewn.dll로 저장한다.
이후 regsvr32.exe 명령어를 사용하여 DLL Emotet 악성코드를 실행한다.

hxxp://eles-tech.com/css/KzMysMqFMs/
hxxp://gonorthhalifax.com/wp-content/yTmYyLbTKZV2czsUO/
hxxps://txpcrescue.com/cgi-bin/5tSO8/
hxxp://hadramout21.com/jetpack-temp/Py/
hxxp://haribuilders.com/zoombox-master/4HYGX/
hxxp://hansen-arnal.com/cp/iiTrAeEtvOwmjjekWgI/

<다수의 DLL 유포지 주소>

2. PE 실행

Emotet DLL 파일 분석

2.1 프로세스

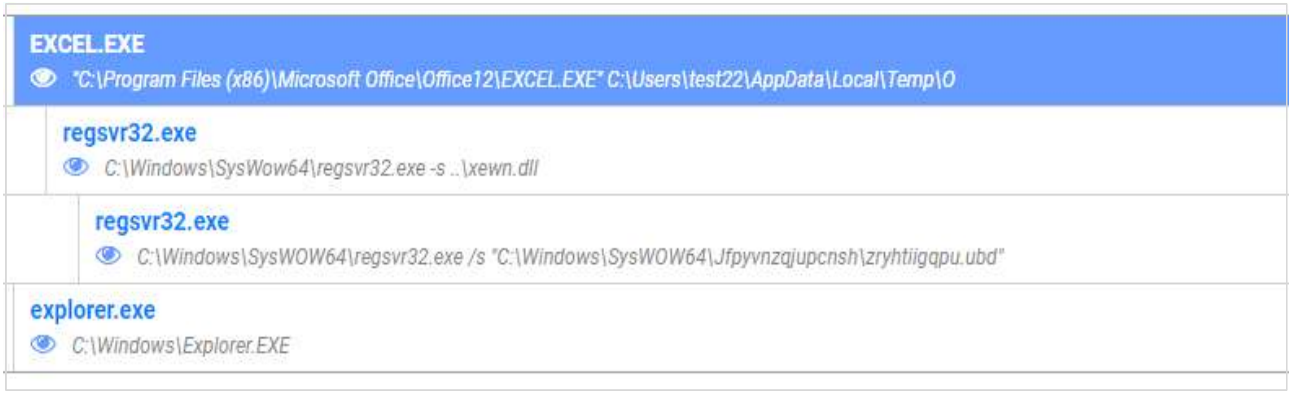

그림 3. DLL 실행 프로세스

실행된 DLL은 특정 경로로 파일을 이동하며, 자식프로세스를 생성한다.

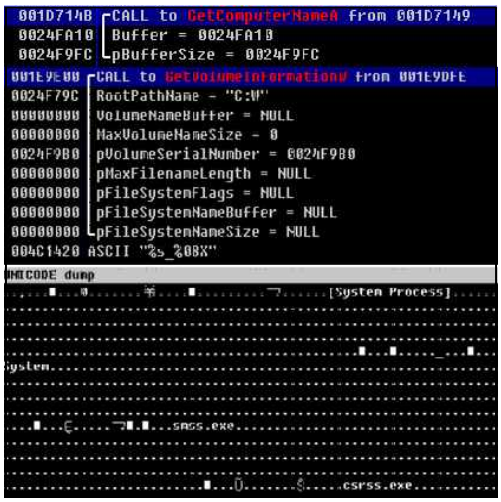

그림 4. 실행중인 프로세스 등 정보수집

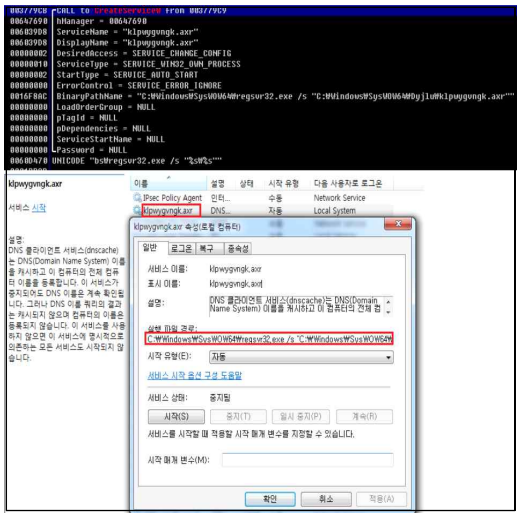

그림 5. 서비스 등록

실행된 DLL파일은 컴퓨터이름, 볼륨 시리얼넘버, 실행중인 프로세스 목록 등을 수집한다.

재부팅 시에도 자동으로 실행될 수 있도록 레지스트리에 등록하며 서비스명은 파일명과 동일하게 생성, 설명란은 기존에 동작중인 서비스의 설명을 랜덤하게 복사하여 사용한다.

2.2 네트워크

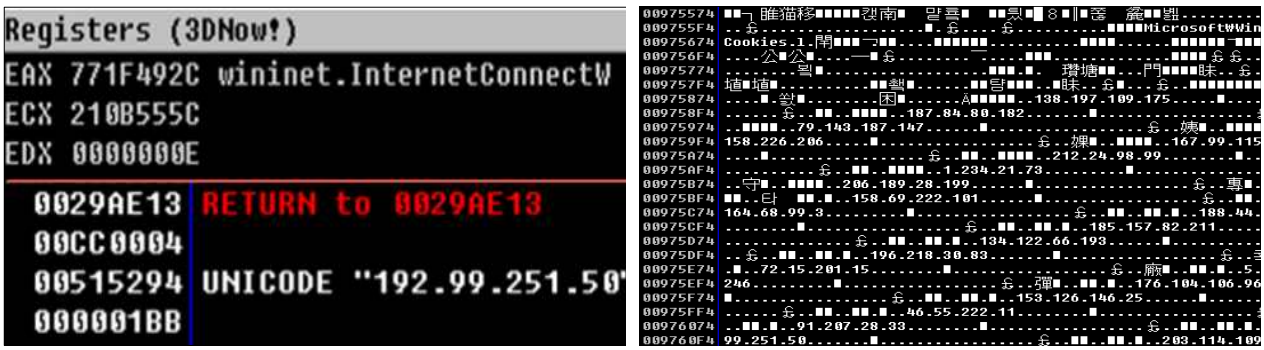

그림 6. C&C 이용 IP

Emotet DLL 파일 실행시 59개의 C&C 서버 주소을 이용하여 접속을 시도하며, 접속에 성공할 시 사용자 정보를 전송하고 공격자로부터 명령을 받아 추가 악성코드 다운로드 등의 악성 행위를 수행할 수 있다.

3. 결론

이메일을 통한 악성코드 유포로 발신인이 불명확한 메일에 대한 사용자의 주의가 필요하겠다.
또한 MS 오피스 문서 파일을 통해 악성코드가 다운로드 및 실행되므로 출처가 분명하지 않은 문서 파일의 매크로 사용을 자제할 필요가 있겠다.

4. 기타

본 악성 문서와 악성코드에서 확인된 IOC 정보

E148A3DEAC1B1FFFC9B34E9877ED936F - MS Excel file
D7AAFBA4171211E3CF2F42800BA94F66 - DLL file

hxxp://eles-tech.com/css/KzMysMqFMs/
hxxp://gonorthhalifax.com/wp-content/yTmYyLbTKZV2czsUO/
hxxps://txpcrescue.com/cgi-bin/5tSO8/
hxxp://hadramout21.com/jetpack-temp/Py/
hxxp://haribuilders.com/zoombox-master/4HYGX/
hxxp://hansen-arnal.com/cp/iiTrAeEtvOwmjjekWgI/

hxxp://138[.]197[.]109[.]175
hxxp://187[.]84[.]80[.]182
hxxp://79[.]143[.]187[.]147
hxxp://216[.]158[.]226[.]206
hxxp://167[.]99[.]115[.]35
hxxp://212[.]24[.]98[.]99
hxxp://1[.]234[.]21[.]73
hxxp://206[.]189[.]28[.]199
hxxp://158[.]69[.]222[.]101
hxxp://164[.]68[.]99[.]3
hxxp://188[.]44[.]20[.]25
hxxp://185[.]157[.]82[.]211
hxxp://134[.]122[.]66[.]193
hxxp://196[.]218[.]30[.]83
hxxp://72[.]15[.]201[.]15
hxxp://5[.]9[.]116[.]246
hxxp://176[.]104[.]106[.]96
hxxp://153[.]126[.]146[.]25
hxxp://46[.]55[.]222[.]11
hxxp://91[.]207[.]28[.]33
hxxp://192[.]99[.]251[.]50
hxxp://203[.]114[.]109[.]124
hxxp://51[.]91[.]7[.]5
hxxp://103[.]70[.]28[.]10
hxxp://209[.]250[.]246[.]206

hxxp://82[.]165[.]152[.]127
hxxp://101[.]50[.]0[.]91
hxxp://151[.]106[.]112[.]196
hxxp://119[.]193[.]124[.]41
hxxp://94[.]23[.]45[.]86
hxxp://51[.]254[.]140[.]238
hxxp://173[.]212[.]193[.]249
hxxp://58[.]227[.]42[.]236
hxxp://212[.]237[.]17[.]99
hxxp://1[.]234[.]2[.]232
hxxp://45[.]118[.]115[.]99
hxxp://110[.]232[.]117[.]186
hxxp://172[.]104[.]251[.]154
hxxp://159[.]65[.]88[.]10
hxxp://185[.]8[.]212[.]13
hxxp://129[.]232[.]188[.]93
hxxp://103[.]43[.]46[.]182
hxxp://103[.]75[.]201[.]2
hxxp://131[.]100[.]24[.]231
hxxp://201[.]94[.]166[.]162
hxxp://45[.]176[.]232[.]124
hxxp://146[.]59[.]226[.]45
hxxp://103[.]132[.]242[.]26
hxxp://209[.]126[.]98[.]206
hxxp://197[.]242[.]150[.]244
hxxp://51[.]91[.]76[.]89
hxxp://160[.]16[.]142[.]56
hxxp://176[.]56[.]128[.]118
hxxp://167[.]172[.]253[.]162
hxxp://189[.]126[.]111[.]200
hxxp://79[.]172[.]212[.]216
hxxp://107[.]182[.]225[.]142
hxxp://50[.]30[.]40[.]196
hxxp://183[.]111[.]227[.]137

* 추가 관련정보는 사이버위협 대응 포털 플랫폼 ZeroBOX 에서 확인하실 수 있습니다.