No. 2

Report

수식편집기 취약점을 통해 유포중인 Formbook 악성코드

2022 · 08 ANALYSIS REPORT

ZERO Co., Ltd.

수식편집기 취약점을 통해 유포중인 Formbook 악성코드 분석 보고서

Formbook 악성코드는 인포스틸러 유형의 악성코드로, 정상프로세스에 인젝션하여 각종 사용자 정보 및 입력 데이터, 클립보드 등을 C2로 전송하는 악성코드이다.

Formbook 악성코드는 대부분 악성 메일을 통해 유포되고 있다. 업무 메일을 가장한 제목으로 꾸준히 유포중에 있으며 첨부된 WORD 파일 실행시 수식편집기 취약점을 악용하여 유포하기도 한다.

1. Non-PE 실행

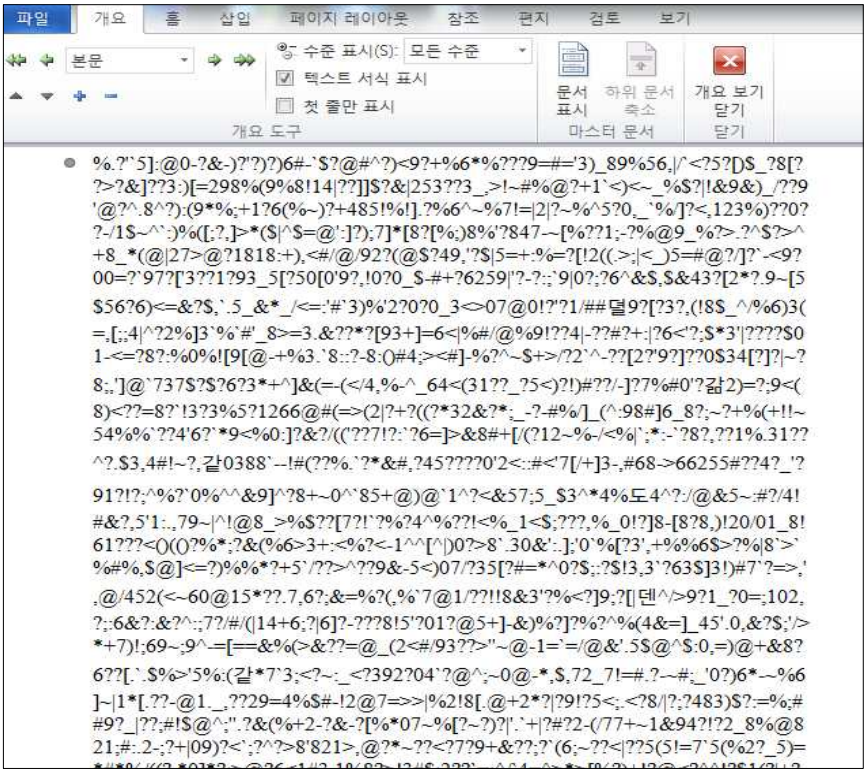

그림 1. WORD 실행 화면

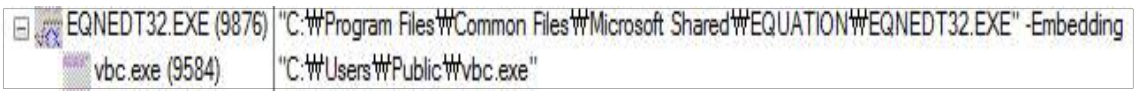

그림 2. 수식 편집기 사용

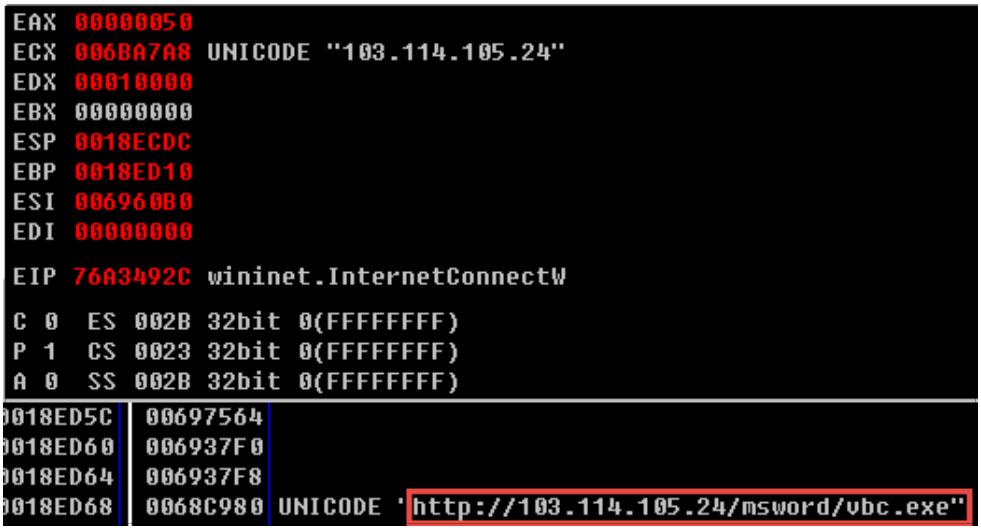

그림 3. 접속 URL

수식편집기 프로그램의 취약점(CVE-2017-11882)을 이용해 특정 서버로부터 악성 파일을 다운로드한다. 현재 접속이 가능한 상태로 Formbook 악성코드가 다운로드 된다.

2. PE 실행

Formbook 파일 분석

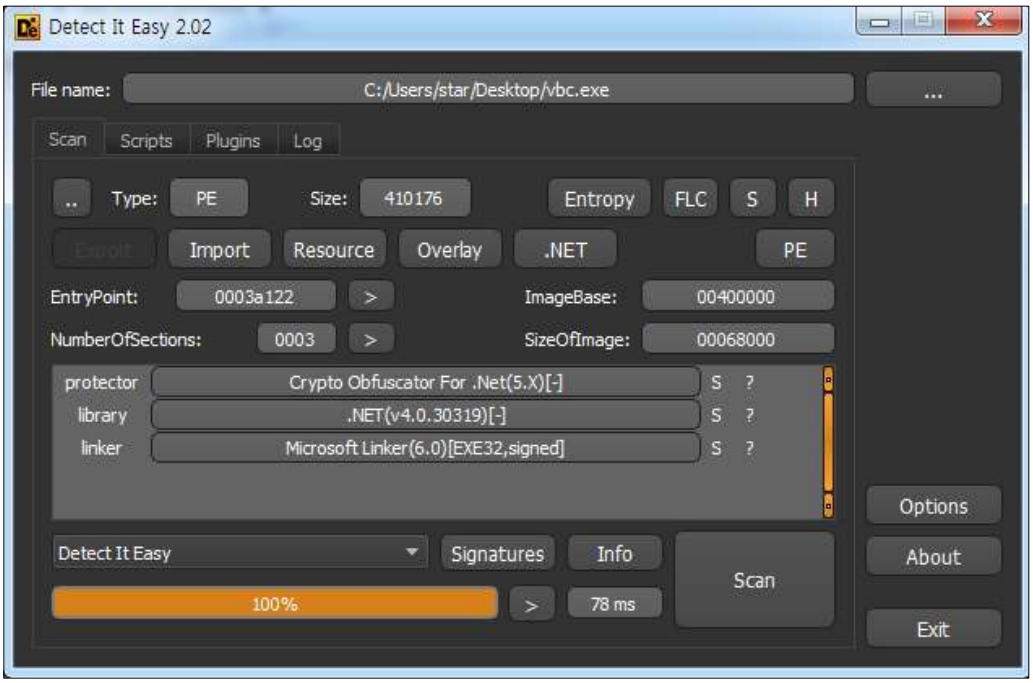

그림 4. Detect It Easy(DiE) 정보

2.1 프로세스

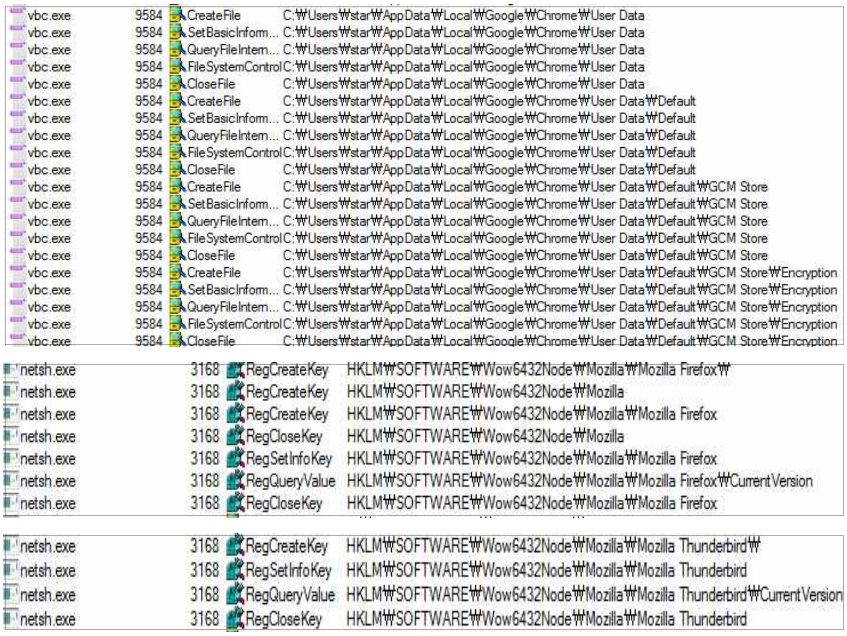

그림 5. 웹 브라우저, 메일 클라이언트 계정정보 수집

다운로드된 vbc.exe 실행후 웹 브라우저 계정정보를 수집하는 것으로 추정되며, 다른 종류의 Formbook에서도 웹 브라우저, 메일 클라이언트 계정정보가 수집되는 것으로 확인된다.

2.2 네트워크

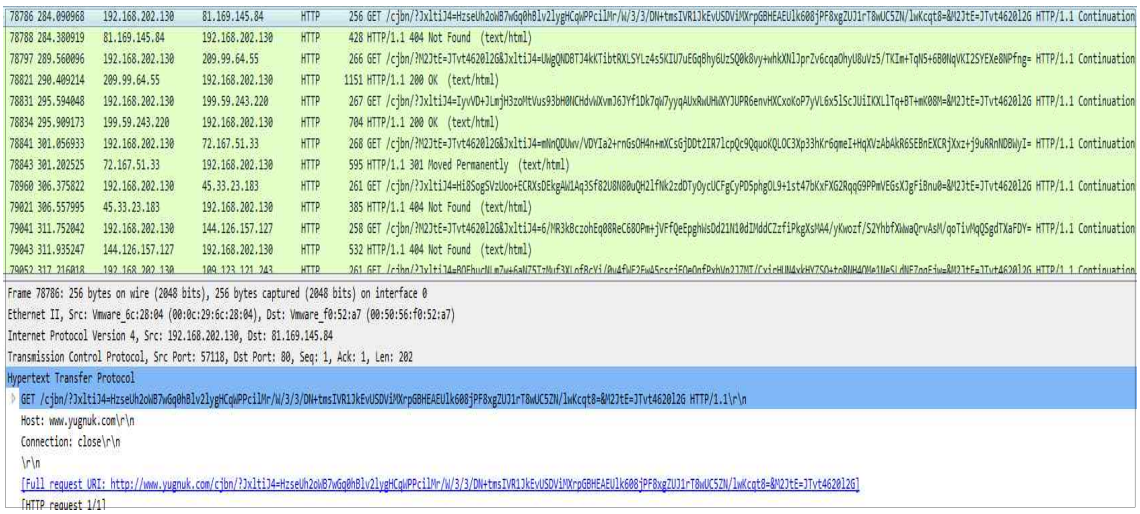

그림 6. C&C 서버 접속 정보

특정 C&C 서버를 통하여 사용자, 웹브라우저 등 수집된 정보를 전송한다.

3. 결론

이메일을 통한 악성코드 유포로 발신인이 불명확한 메일에 대한 사용자 주의가 필요하겠다.

또한 Word 파일 수식 편집기 취약점을 통해 악성코드가 다운로드 및 실행되므로 출처가 분명하지 않은 Word 파일 실행을 자제할 필요가 있다.

4. IoC 정보

www.doc / md5 5FB9FA4EF5C7A77400A888C307230082 doc
vbc.exe / md5 120BBFBA12A460A387467D3D4E558A8B exe

hxxp://www[.]atama[.]engineering/cjbn/?_DKdFz=wwYd9s1PhWDpqmjLY6K8aFynxAr0zZAcfatdMZ7LxDCbB30TkBsKnVLUlfW8ihTIpTvuS4AsNYhWgFScHOZ0ntFjDhWMCBF4R2S3v5o=&rL0=d8qtmDrhzHx
hxxp://www[.]yugnuk[.]com/cjbn/?_DKdFz=HzseUh2oWB7wGq0mPkfMnE8HJaWMPaelMr/W/3/3/DN+tmsIVR1JkEvUSDViMXrpGBHEAEUlk608jMpk6hNUNBLV7kQ16owJy0Gf8rU=&rL0=d8qtmDrhzHx
hxxp://www[.]vilkahoofre[.]xyz/cjbn/?_DKdFz=BOEhucNLmZw+6aNe3SD2sprXAYfCcee/0v4fWE2FwA5rsrjEOeQnfPxhVn2JZMT/CxirHUN4xkHYZR8mmpFNDMwKZhJpR6g7TdmpTlY=&rL0=d8qtmDrhzHx
hxxp://www[.]uk-exxonmobil[.]com/cjbn/?_DKdFz=zTKbkOOwsEMH9NlXj0zzhobSxDp9HnG8c4Mfdq5DrJLcK8N980Ax076jsATXWVJd9FsOU2We6lxDyVRz+U3VNoF8iUULU9pjsKvA9WU=&rL0=d8qtmDrhzHx
hxxp://www[.]indigocreditcards[.]com/cjbn/?_DKdFz=IyvVD+JLmjH3zoMqbvcH1tb0GyHevQrvmJ6JYf1Dk7qW7yyqAUxRwUHWXYJUPR6envHXCxoKoP7yVIWpykGcNgCONDPSQbD3E6qJi6k=&rL0=d8qtmDrhzHx
hxxp://www[.]daniel-gerard[.]com/cjbn/?_DKdFz=3Tav2a3a8Qp1V2Az9A+tZljLPWvpaeVNIS3CRwknMo9xqkwkpiFRKo5wEzE8rirMRuyVE3pvD0radIY65TbIZGMtd9RmNYkgXZTaJrw=&rL0=d8qtmDrhzHx
hxxp://www[.]weddinggayfriendly[.]com/cjbn/?_DKdFz=PBoR/ipJgfM3JzDbiMlt317GkUwW2BccjhHSu663aMtOL05dzR/iud/TIcitK1IkVf+ojexym9Bb39ODDcU0p7gX9USBawSRphbA77Y=&rL0=d8qtmDrhzHx
hxxp://www[.]moralincense[.]directory/cjbn/?_DKdFz=mNnQDUwv/VDYIa25lm2WMxkn1WXBsAfDDt2IR7lcpQc9QquoKQLOC3Xp33hKr6qmeI+HqXVzAbAkR5+cKmQXGlDR2n6U+fsnwJPCA0g=&rL0=d8qtmDrhzHx
hxxp://www[.]symbolsdecoded[.]com/cjbn/?_DKdFz=b1lfdMeokRhLMFmDL+6QnXF1HtBC/782RGSOWzpE+0IGD+o5IQiz5hMUHjomSuOIU+pmV7JF2uB9K8U/MlYuqpVgzwZja3B6XqVIFNA=&rL0=d8qtmDrhzHx

hxxp://www[.]mikrobol[.]com/cjbn/?_DKdFz=6/MR3kBczohEq08WQDKGM56+olFcQY4pghWsDd21N10dIMddCZzfiPkgXsMA4/yKwozf/S2YhbfXWz2IguUsILKuU2r7phvWKXbZTFw=&rL0=d8qtmDrhzHx
hxxp://www[.]namastechocolate[.]com/cjbn/?_DKdFz=UWgQNDBTJ4kKTibqfW7oa9v4nJKLU9SEGqBhy6UzSQ0k8vy+whkXNlJprZv6cqaOhyU8uVz5/TKIm9/yG4q6FAtsSeMBRp5hJ4BMJhI=&rL0=d8qtmDrhzHx
hxxp://www[.]vitaminb12power[.]com/cjbn/?_DKdFz=yf10IpFsug0ZRn2xtAGlElJp+P3LqO4ebEkYSmBRh2t7w8mUfIKSx8aO4BQFDmQMuEPYsENA5aaKHUDpngkxr+azfXtUN1froVG3H9M=&rL0=d8qtmDrhzHx
hxxp://www[.]wallet-polygons[.]space/cjbn/?_DKdFz=lryaHGMQz4MuCsvNMuBjX0YuYy0rizfXvATt0sqhZjAu7Lx1USNqSrQ73djU1uvE9l+/EOx5kycmg1HQ6tQxKs5IYLfnAuJCIee6UMQ=&rL0=d8qtmDrhzHx
hxxp://www[.]advancedeventsystemsd[.]com/cjbn/?_DKdFz=L2m139IdwFQM4YjRimZO9yU9NT3WhCoy5LwfeJ+vwQhRie3cxv7zT6Nx4kPKLHx4pQBKT5tJTg7iX3Kya3ZIlk/WUe9mUJPNPt/jeSw=&rL0=d8qtmDrhzHx
hxxp://www[.]insectore[.]co[.]uk/cjbn/?_DKdFz=Hi8SogSVzUoo+ECWZtz+mWcW+wq0SZA2U8N80uQH2lfNk2zdDTyOycUCFgCyPD5phgOL9+1st47bKypPN3FquydJIyRzFdq/3BuCxoc=&rL0=d8qtmDrhzHx
hxxp://www[.]qrupeocajarual[.]com/cjbn/?_DKdFz=+9yLynGFwfsBmw1HADDFEc18Ta9EiaLz5Iz/V5jWpHnylC+m84WxH7LdBMBoc3G91DlV+5/CN96Lbbt5dK/EFomhuyengD5dE+FPq50=&rL0=d8qtmDrhzHx

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