Document Macro Malware II

Encapsulated PostScript Vulnerability GhostScript

malwares.com™

2019.1.14 Pvgodd

Document Macro Malware

PostScript

vs

Encapsulated PostScript

Document Macro Malware

북한 사이버 공격그룹, 세금 관련 한글문서 이용해 국내 가상화폐 기업 공격

파이어아이 "국내 가상 화폐 서비스 제공업체들 타깃으로 공격" 추정

길민권 기자 mkgil@dailysecu.com 2017년 09월 12일 화요일

폰트 + −

세무조사 준비서류

준비할 사항

1. 회사연혁 및 본점, 지점, 공장 조직도

2. 업종별 업무(영업) 흐름도

3. 대표이사 및 주요 임직원, 주주 현황

4. 법인세, 부가가치세, 원천세 등 각종 세무 신고서

5. 전표 및 증빙철

6. 계정별 원장(출력물 또는 전산자료) 및 거래처별 원장

7. 세금계산서, 계산서 및 거래명세서

8. 어음 수불대장, 재고자산 관리대장 등

9. 주식변동조사 포함 시 주식변동 내역을 입증하는 주식 양수.도 계약서, 신고서 및 자금출처 관련서류

10. 정관, 사규, 이사회 회의록 등 회사규정 및 의사결정에 관한 자료

11. 법인 통장 또는 예금 거래명세서(사업용계좌)

12. 기타 법인세 등 각종세무신고 시 기초자료가 되는 근거서류

▲ 세무조사준비서류.hwp. 파이어아이 제공

파이어아이 측은 스피어 피싱 이메일 및 관련 미끼문서 확인 결과, TEMP.Hermit공격자들이 국내 환전 및 중개사무소와 같은 가상 화폐 서비스 제공업체들을 노렸을 것으로 판단하고 있다.

이러한 활동은 가상 통화를 활용해 돈을 송금하거나 가상 화폐 서비스를 직접적으로 침해하려는 의도였을 가능성이 높다. 국제적 제재로 인해 거세진 압력 때문에 북한 공격자들은 금전적 목적으로 공격을 감행해 왔다. 그러나 이번 가상 화폐 서비스가 피해 대상의 일부였는지 다른 조직도 공격 대상에 있었는지 명확하게 밝혀지지 않았다.

북한 공격자들이 가상 화폐를 어떻게 활용하는지 아직 밝혀진 바가 없다. 다른 화폐나 중앙 은행에 의해 관리되고 추적될 수 있는 통화에 비해 가상 화폐는 비교적 독립적이고 익명으로 거래된다. 특히 국가적 제재가 계속 강화되는 가운데 가상 화폐의 이러한 특징은 북한 공격자들에게 매력적인 매개체로 비춰졌을 가능성이 높다. 이번 공격의 북한 용의자들은 지난 2 월말 발생한 비트코인 뉴스 웹사이트의 전략적 웹 침해 사건과 같이 앞서 가상 화폐 사이트를 목표로 삼아왔다.

금융감독원을 사칭하는 스피어 피싱 이메일이 서울에 위치한 가상 화폐 중개사무소 관리자에게 보내졌으며, 스피어피싱 이메일에는 '환전_해외송금_한도_및_제출서류.hwp'라는 악성 첨부파일이 포함됐다. 파이어아이는 다음과 같은 파일 이름의 미끼 문서도 확인했다. 아래 문서는 각별히 주의해야 한다.

-세무조사준비서류.hwp
-법인(개인)혐의거래보고내역.hwp 및 법인(개인)혐의거래보고내역.hwp
-납세담보변경요구서.hwp

관련된 샘플들은 약간씩 다른 기술을 사용했지만 미끼 메타데이터나 유사 미끼 내용을 기반으로 한 동일한 공격 캠페인의 일부로 추정된다. 가상 화폐 브로셔를 사용한 미끼문서는 공격이 가상 화폐 투자에 대한 이해관계나 관심이 있는 개인을 대상으로 이루어졌음을 나타내고 있다. 다음 파일들은 CVE-2017-0262 취약점을 악용해 PEACHPIT 멀웨어를 전파했다.

-2017년5월까지감지된유사수신행위와법률적조치.docx
-국내가상화폐의유형별현황및향후전망.hwp

Document Macro Malware

- HWP Format
  - OLE Object
    - **Document Video Sound Graph Chart Table**
    - **Linked Object**

      Points for Source File Data
    - **Embeded Object**

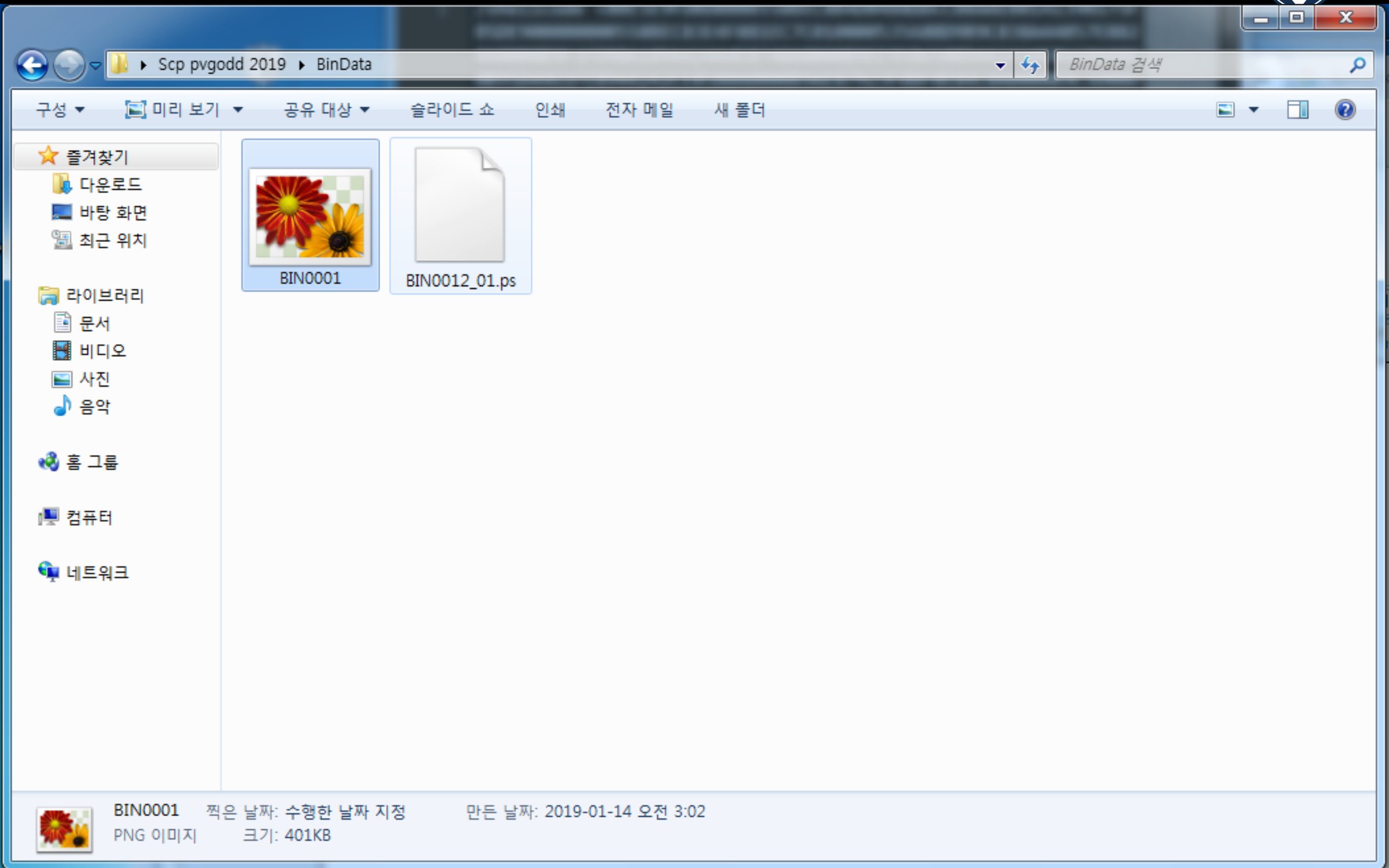
      Copy data from source file

Document Macro Malware

Storage Stream

설명	구별 이름	길이(바이트)	레코드 구조	압축/암호화
파일 인식 정보	FileHeader	고정		
문서 정보	DocInfo	고정	√	√
본문	BodyText Section0 Section1 ...	가변	√	√
문서 요약	\005HwpSummaryInformation	고정		
바이너리 데이터	BinData BinaryData0 BinaryData1 ...	가변		√
미리보기 텍스트	PrvText	고정		
미리보기 이미지	PrvImage	가변		
문서 옵션	DocOptions _LinkDoc DrmLicense ...	가변		
스크립트	Scripts DefaultJScript JScriptVersion ...	가변		
XML 템플릿	XMLTemplate Schema Instance ...	가변		
문서 이력 관리	DocHistory VersionLog0 VersionLog1 ...	가변	√	√

Document Macro Malware



Document Macro Malware

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	02	65	00	00	00	E3	08	02	00	00	00	4B	9B	F4	...e...ã.....K›ô
00000020	9C	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	œ....sRGB.®Î.é..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA..±..üa...
00000040	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs...Ã...Ã.Ç
00000050	6F	A8	64	00	00	FF	A5	49	44	41	54	78	5E	EC	9D	05	o¨d..ÿ¥IDATx^ì..
00000060	78	54	E7	BA	B6	57	DC	26	E3	EE	EE	13	77	4F	20	48	xTç°¶WÜ&ãîî.wO H
00000070	B0	10	48	82	43	71	77	28	EE	14	5A	A0	A5	02	2D	52	°.H‚Cqw(î.Z ¥.-R
00000080	AC	94	52	2F	15	5A	4A	DD	DD	DD	BD	D4	71	88	31	FF	¬”R/.ZJÝÝÝ½Ôqˆ1ÿ
00000090	F3	AD	6F	B2	18	02	ED	EE	39	E7	3F	25	3D	AC	7D	BD	ó.o²..íî9ç?%=¬}½

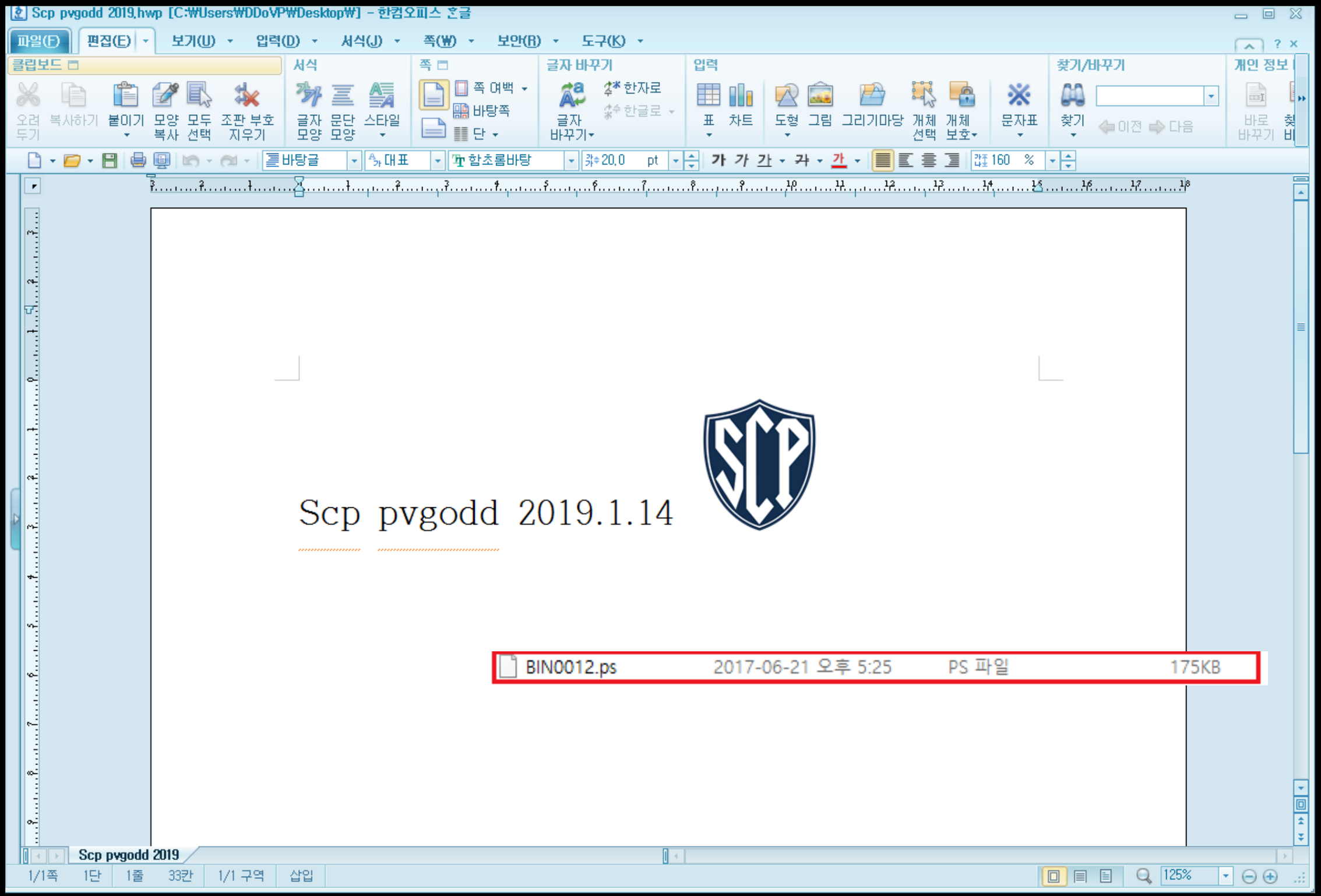
원본 그림파일 데이터

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	34	56	79	3C	54	EB	FF	67	1A	DF	6B	C2	55	A3	C8	72	4Vy<Tëÿg.ßkÂU£Èr
00000010	B3	CD	19	4D	86	93	25	DB	B5	64	8B	71	48	4D	C9	DA	³Í.M†“%Ûµd‹qHMÉÚ
00000020	20	B4	88	B2	95	A5	EC	22	B9	96	06	73	AC	59	EE	50	´ˆ²•¥ì"¹–.s¬YîP
00000030	52	62	2C	4D	85	29	33	B2	85	D2	E2	72	15	62	CC	95	Rb,M…)3²…Òâr.bÌ•
00000040	B8	63	2B	CB	30	BF	D3	7D	BD	7E	7F	9C	E7	3C	CF	EB	¸c+Ë0¿Ó}½~.œç<Ïë
00000050	75	CE	F3	7C	DE	9F	F7	E7	FD	FE	3C	E9	C7	8F	D9	49	uÎó|ÞŸ÷çýþ<éÇ.ÙI
00000060	ED	54	D8	29	22	22	22	45	B2	B7	21	8B	88	A0	02	90	íTØ)"""E²·!‹ˆ ..
00000070	F9	94	38	0A	19	A1	E2	95	12	E4	25	1A	4E	B6	B3	12	ù”8..¡â•.ä%.N¶³.
00000080	A9	1B	50	9A	45	16	E8	F3	96	4E	96	22	22	0D	D9	12	©.PšE.èó–N–"".Ù.
00000090	02	5F	31	64	8D	09	B1	77	0F	17	11	F9	95	FD	F3	11	._1d..±w...ù•ýó.

BIN0001.png 파일 데이터

바이너리 데이터	BinData BinaryData0 BinaryData1 ...	가변		√

Document Macro Malware



Document Macro Malware

File Options View Process Find DLL Users Help

Process	PID	Private Byt...	Working S...	CPU	Description	Company Name
System Idle Process	0	0 K	8 K	84.78		
System	4	268 K	50,048 K	0.33		
csrss.exe	568	852 K	1,280 K	< 0....		
wininit.exe	632	756 K	420 K			
csrss.exe	640	1,028 K	4,540 K	0.14		
winlogon.exe	688	1,272 K	1,920 K			
MpCmdRun.exe	3236	3,060 K	6,388 K			
explorer.exe	3452	31,828 K	59,588 K	0.33	Windows 탐색기	Microsoft Corpora
OneDrive.exe	1108	6,884 K	7,164 K		Microsoft OneDrive	Microsoft Corpora
procexp.exe	4648	11,180 K	19,296 K	3.49	Sysinternals Process E...	Sysinternals - www
Tcpview.exe	5176	7,076 K	11,744 K	0.77		
Hwp.exe	4428	69,420 K	83,012 K		Hancom Office Hanwo...	Hancom Inc(HNC).
HimTrayIcon.exe	308	996 K	5,768 K	0.01		
gswin32c.exe	5256	9,828 K	11,964 K			
conhost.exe	5464	9,808 K	9,604 K	0.01	Console Window Host	Microsoft Corpora
Windows10UpgraderApp...	5792	23,668 K	9,792 K	7.49		
MpCmdRun.exe	4588	1,656 K	5,556 K			

Name	Description	Company Name	Path
comctl32.dll	User Experience Controls Li...	Microsoft Corporation	C:₩Windows₩WinSxS₩x86_microsoft.window
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:₩Windows₩System32₩comdlg32.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:₩Windows₩System32₩gdi32.dll
gsdll32.dll			C:₩Program Files₩Hnc₩Common80₩ImgFilte
gswin32c.exe			C:₩Program Files₩Hnc₩Common80₩ImgFilte
imm32.dll	Multi-User Windows IMM3...	Microsoft Corporation	C:₩Windows₩System32₩imm32.dll
kernel.appcore....	AppModel API Host	Microsoft Corporation	C:₩Windows₩System32₩kernel.appcore.dll