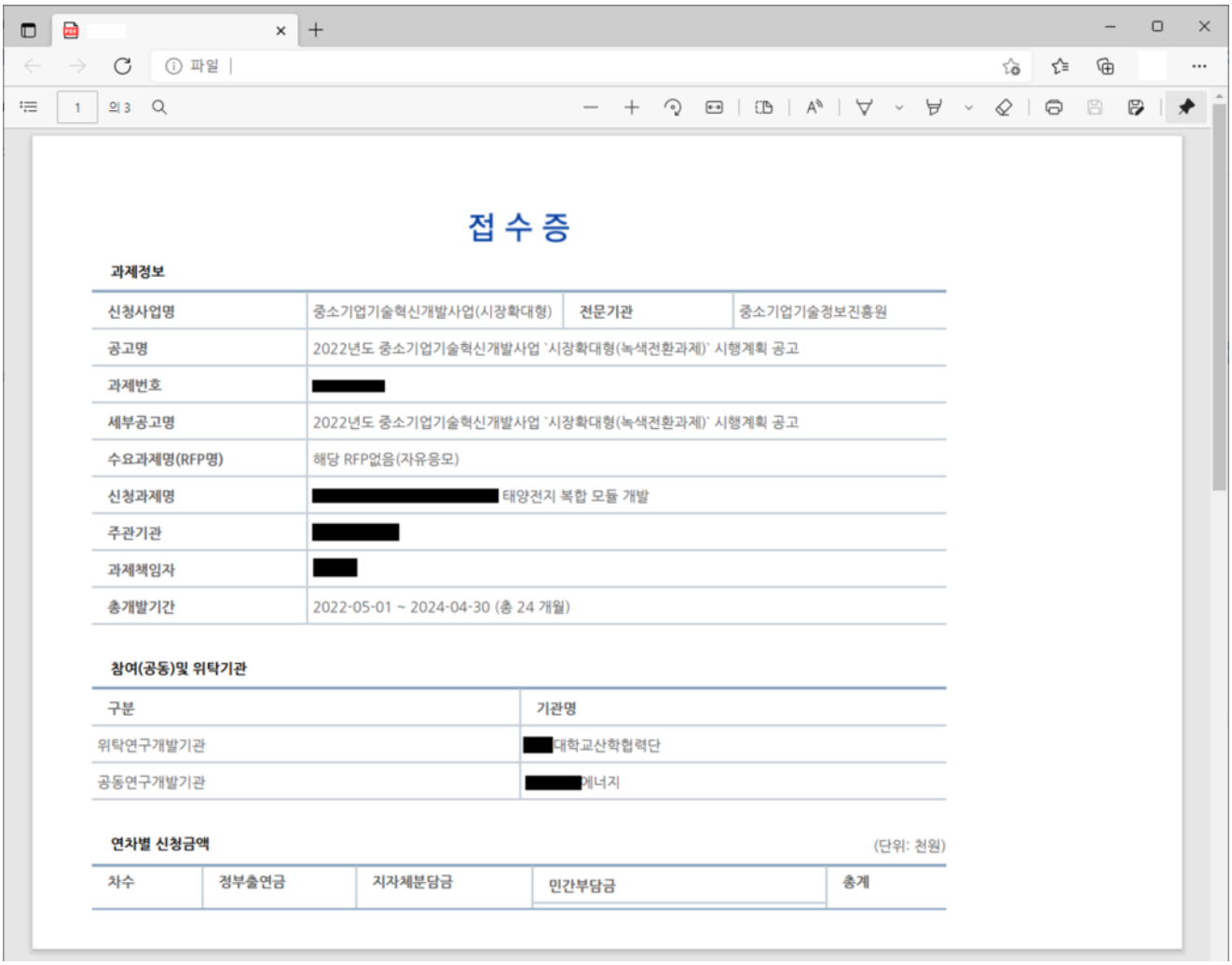
VBS Script Disguised as PDF File Being Distributed (Kimsuky)

asec.ahnlab.com/en/33032/

March 28, 2022

On March 23rd, the ASEC analysis team has discovered APT attacks launched by an attack group presumed to be Kimsuky, and they targeted certain Korean companies. Upon running the script file with the VBS extension, the malware runs the innocuous PDF file that exists internally to trick the user into thinking that they opened an innocuous document file and uses a malicious DLL file to leak information. Taking PDF file into consideration, it seems the attacker is targeting precise-refinement industries. See the figure below for details of PDF file.

> Filename: Application receipt-Small business technology innovation and development project_Market expansion_Green conversion_S???????.pdf.vbs



접 수 증

과제정보

신청사업명	중소기업기술혁신개발사업(시장확대형)	전문기관	중소기업기술정보진흥원
공고명	2022년도 중소기업기술혁신개발사업 `시장확대형(녹색전환과제)` 시행계획 공고		
과제번호	[redacted]		
세부공고명	2022년도 중소기업기술혁신개발사업 `시장확대형(녹색전환과제)` 시행계획 공고		
수요과제명(RFP명)	해당 RFP없음(자유응모)		
신청과제명	[redacted] 태양전지 복합 모듈 개발		
주관기관	[redacted]		
과제책임자	[redacted]		
총개발기간	2022-05-01 ~ 2024-04-30 (총 24 개월)		

참여(공동)및 위탁기관

구분	기관명
위탁연구개발기관	[redacted]대학교산학협력단
공동연구개발기관	[redacted]에너지

연차별 신청금액 (단위: 천원)

차수	정부출연금	지자체분담금	민간부담금	총계

Figure 1. Innocuous PDF file used as bait

The team presumes this to be the work of the Kimsuky group due to the following evidence.

- Malware is run via ‘regsvr32.exe’ similar to the existing AppleSeed
- kro.kr domain, known to be used by Kimsuky, is used as C&C
- When relaying attacker’s commands, commands such as tasklist, net user, and systeminfo are run

The attacker also added ‘.pdf’ in front of the extension to trick users. For many ordinary users, ‘Hide extensions for known file types’ is enabled by default (see Figure 2), resulting in the users mistaking the file for a PDF file even though it is a VBS file. Ultimately, when the user runs the VBS, a malicious activity commences in parallel with the execution of the PDF file.

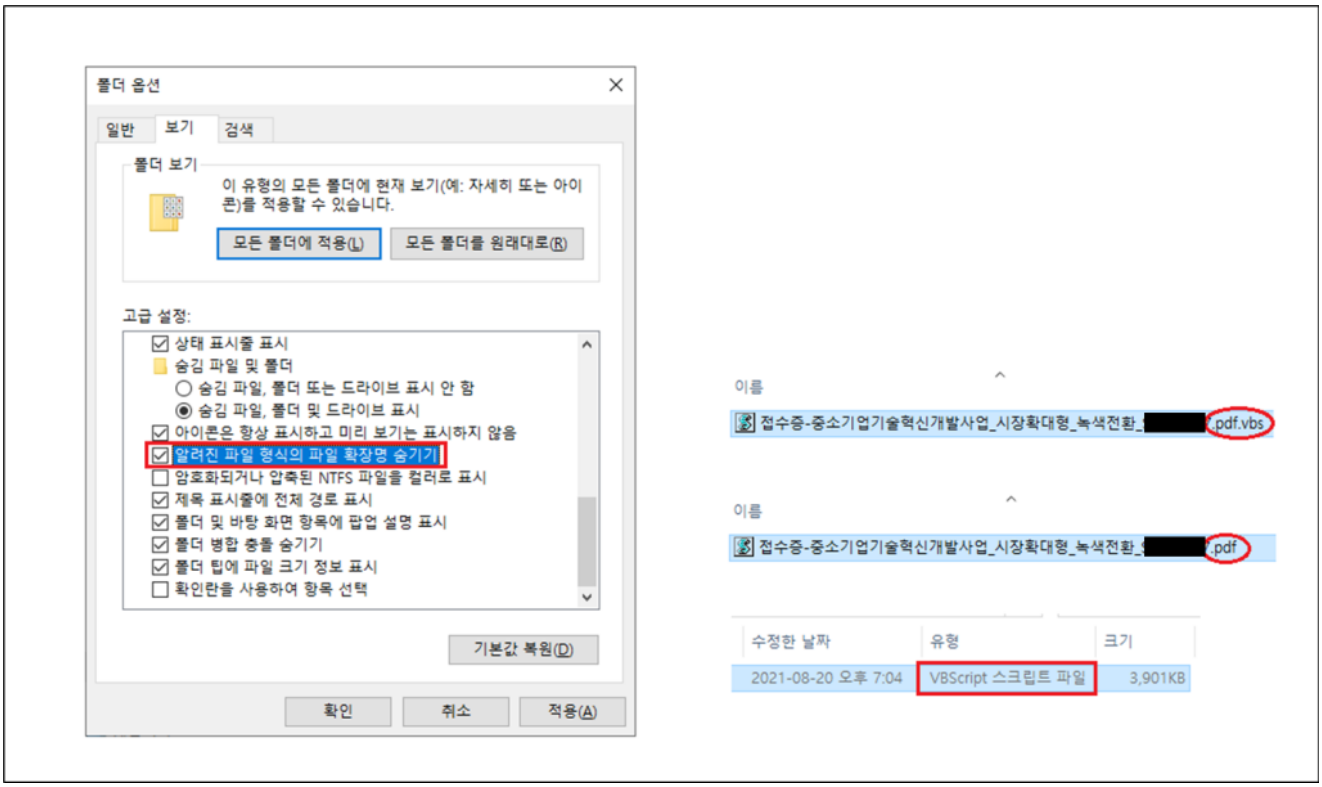


Figure 2. Feature of hiding file extension

The malicious VBS creates and runs the innocuous PDF file in the path where the VBS was run, and Base64-encoded DLL in the path 'C:\ProgramData'. The filename of the DLL created by the internal code is random as shown below.

- %ALLUSERSPROFILE%\tewl8.aqdzkz
- %ALLUSERSPROFILE%\ltbpq.brv5la
- %ALLUSERSPROFILE%\ihjq6.xvcdkk

The malicious DLL that is run at the end creates the cmd.exe process and waits for the pipe communication with the C&C server. The confirmed attacker commands during the standby are as follows.

- systeminfo command
- tasklist command
- whoami command
- net user command

AhnLab is continuously monitoring and responding to such APT attacks, and users must disable 'Hide extensions for known file types' that is enabled by default (see Figure 2) to prevent being tricked by such a technique.

AhnLab's anti-malware software, V3, is currently detecting and blocking the files using the following aliases.

[IOC]

[MD5]
– Innocuous PDF file: b3c7df17420d48f61bbfcf2bac3ae4a3
– VBS file: 64cbd6f435538175dc06ea4b84cba46d
– Final DLL (backdoor): 856072827cec7b74ead3ce40e55bd8d1
– DLL created by VBS: 3ea9b50289aecccc7ffd04fa814c1a5c

[**Detection Name (Engine version)]**
– VBS file: Dropper/VBS.Akdoor (2022.03.24.00)
– Final DLL (backdoor): Trojan/Win.Kimsuky.C5025515 (2022.03.24.00)
– DLL created by VBS: Trojan/Win.Kimsuky.C5025516 (2022.03.24.00)

[C&C]
– hxxps://regular.winupdate.kro.kr/index.php

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

Categories:Malware Information

Tagged as:APT, Kimsuky