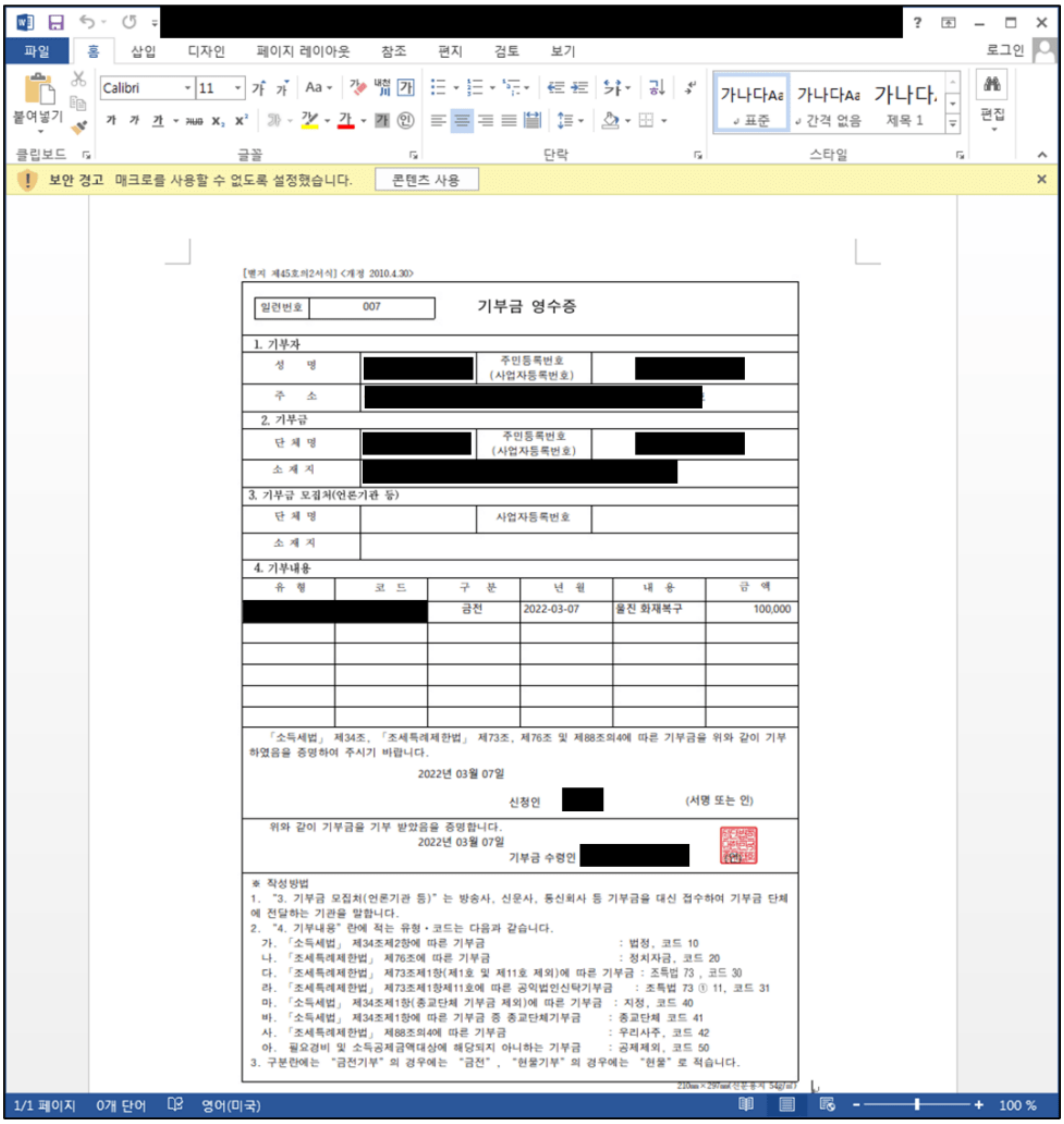
Posted on April 1, 2022

APT Attacks Using Word File Disguised as Donation Receipts for Uljin Wildfire (Kimsuky)

At the beginning of March this year, a wildfire broke out in the Samcheok and Wuljin area, and numerous people from all over Korea donated to help the victims and restore the damages. Amidst such a situation, the ASEC analysis team discovered the attacker's attempt at launching APT attacks disguised as donation receipts for the Uljin wildfire.



보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

[별지 제45호의2서식] <개정 2010.4.30>

일련번호	007

기부금 영수증

1. 기부자

성 명	[redacted]	주민등록번호 (사업자등록번호)	[redacted]
주 소	[redacted]		

2. 기부금

단 체 명	[redacted]	주민등록번호 (사업자등록번호)	[redacted]
소 재 지	[redacted]		

3. 기부금 모집처(언론기관 등)

단 체 명		사업자등록번호	
소 재 지			

4. 기부내용

유 형	코 드	구 분	년 월	내 용	금 액
[redacted]	[redacted]	금전	2022-03-07	울진 화재복구	100,000

「소득세법」 제34조, 「조세특례제한법」 제73조, 제76조 및 제88조의4에 따른 기부금을 위와 같이 기부하였음을 증명하여 주시기 바랍니다.

2022년 03월 07일

신청인 [redacted] (서명 또는 인)

위와 같이 기부금을 기부 받았음을 증명합니다.

2022년 03월 07일

기부금 수령인 [redacted] (인)

※ 작성방법

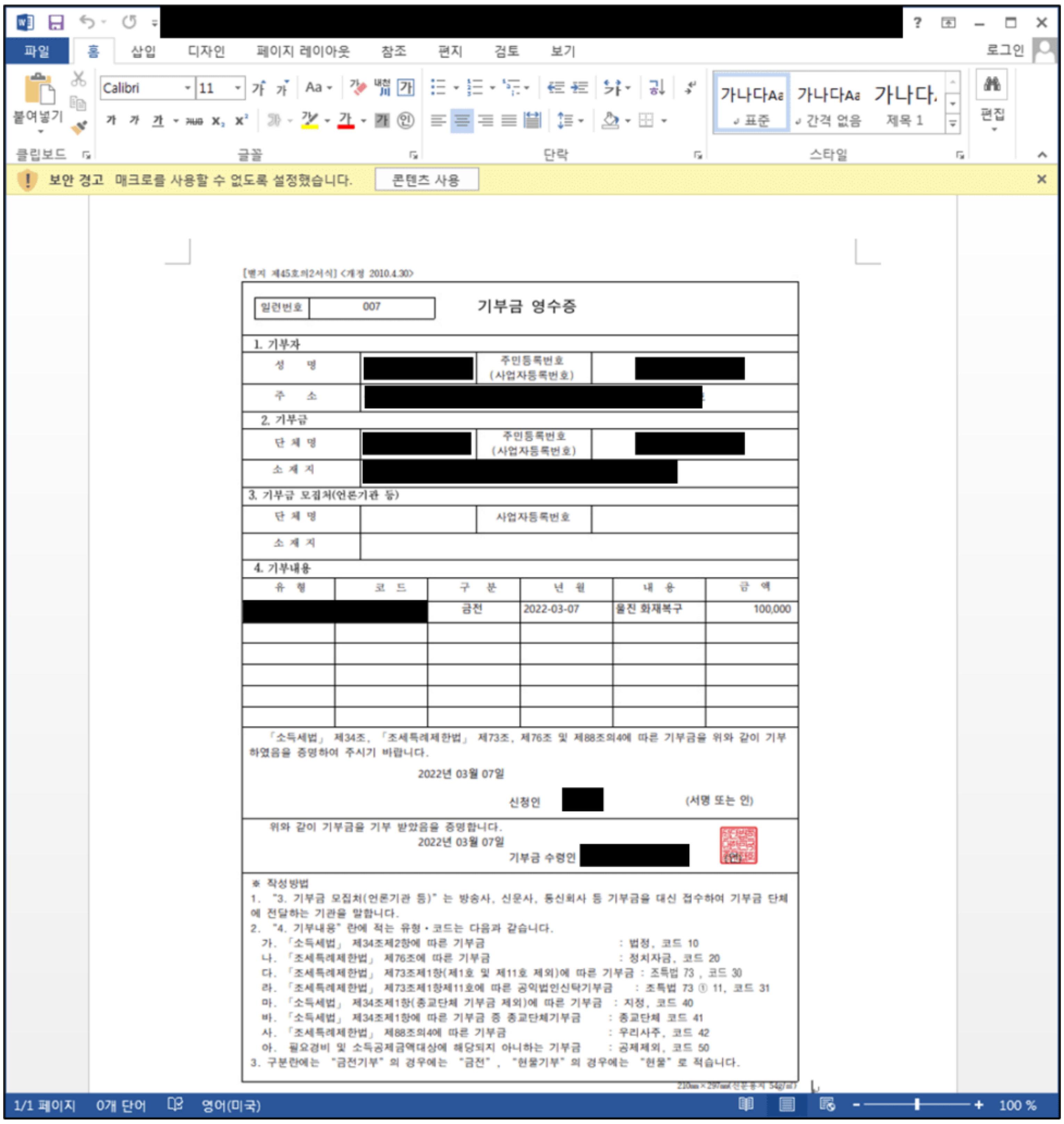
1. "3. 기부금 모집처(언론기관 등)" 는 방송사, 신문사, 통신회사 등 기부금을 대신 접수하여 기부금 단체에 전달하는 기관을 말합니다.

2. "4. 기부내용" 란에 적는 유형・코드는 다음과 같습니다.

가. 「소득세법」 제34조제2항에 따른 기부금	: 법정, 코드 10
나. 「조세특례제한법」 제76조에 따른 기부금	: 정치자금, 코드 20
다. 「조세특례제한법」 제73조제1항(제1호 및 제11호 제외)에 따른 기부금	: 조특법 73 , 코드 30
라. 「조세특례제한법」 제73조제1항제11호에 따른 공익법인신탁기부금	: 조특법 73 ① 11, 코드 31
마. 「소득세법」 제34조제1항(종교단체 기부금 제외)에 따른 기부금	: 지정, 코드 40
바. 「소득세법」 제34조제1항에 따른 기부금 중 종교단체기부금	: 종교단체 코드 41
사. 「조세특례제한법」 제88조의4에 따른 기부금	: 우리사주, 코드 42
아. 필요경비 및 소득공제금액대상에 해당되지 아니하는 기부금	: 공제제외, 코드 50

3. 구분란에는 "금전기부" 의 경우에는 "금전" , "현물기부" 의 경우에는 "현물" 로 적습니다.

210㎜×297㎜(신문용지 54g/㎡)



보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

[별지 제45호의2서식] <개정 2010.4.30>

일련번호	007	기부금 영수증			
1. 기부자					
성 명	[redacted]	주민등록번호 (사업자등록번호)	[redacted]		
주 소	[redacted]				
2. 기부금					
단 체 명	[redacted]	주민등록번호 (사업자등록번호)	[redacted]		
소 재 지	[redacted]				
3. 기부금 모집처(언론기관 등)					
단 체 명		사업자등록번호			
소 재 지					
4. 기부내용					
유 형	코 드	구 분	년 월	내 용	금 액
[redacted]	[redacted]	금전	2022-03-07	울진 화재복구	100,000

「소득세법」 제34조, 「조세특례제한법」 제73조, 제76조 및 제88조의4에 따른 기부금을 위와 같이 기부하였음을 증명하여 주시기 바랍니다.

2022년 03월 07일

신청인 [redacted] (서명 또는 인)

위와 같이 기부금을 기부 받았음을 증명합니다.

2022년 03월 07일

기부금 수령인 [redacted] (인)

※ 작성방법

1. "3. 기부금 모집처(언론기관 등)" 는 방송사, 신문사, 통신회사 등 기부금을 대신 접수하여 기부금 단체에 전달하는 기관을 말합니다.

2. "4. 기부내용" 란에 적는 유형・코드는 다음과 같습니다.

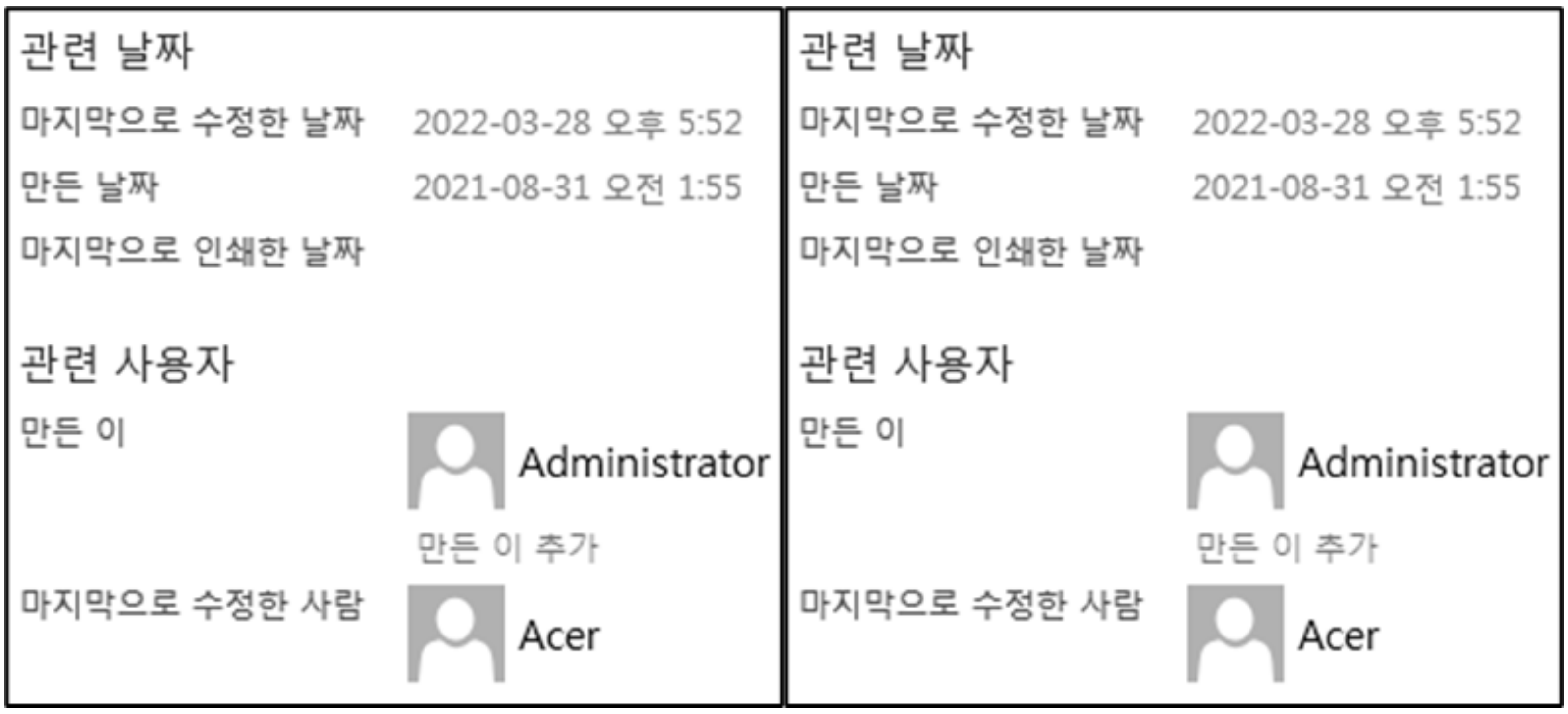
가. 「소득세법」 제34조제2항에 따른 기부금 : 법정, 코드 10
나. 「조세특례제한법」 제76조에 따른 기부금 : 정치자금, 코드 20
다. 「조세특례제한법」 제73조제1항(제1호 및 제11호 제외)에 따른 기부금 : 조특법 73 , 코드 30
라. 「조세특례제한법」 제73조제1항제11호에 따른 공익법인신탁기부금 : 조특법 73 ① 11, 코드 31
마. 「소득세법」 제34조제1항(종교단체 기부금 제외)에 따른 기부금 : 지정, 코드 40
바. 「소득세법」 제34조제1항에 따른 기부금 중 종교단체기부금 : 종교단체 코드 41
사. 「조세특례제한법」 제88조의4에 따른 기부금 : 우리사주, 코드 42
아. 필요경비 및 소득공제금액대상에 해당되지 아니하는 기부금 : 공제제외, 코드 50

3. 구분란에는 "금전기부" 의 경우에는 "금전" , "현물기부" 의 경우에는 "현물" 로 적습니다.

210mm×297mm(신문용지 54g/㎡)

Figure 1. Donation receipt (OOO).doc

The file was created on March 28th, and its author's name is the same as the author (Acer) that was introduced in the previous ASEC blog.



관련 날짜
마지막으로 수정한 날짜 2022-03-28 오후 5:52
만든 날짜 2021-08-31 오전 1:55
마지막으로 인쇄한 날짜

관련 사용자
만든 이 Administrator
만든 이 추가
마지막으로 수정한 사람 Acer

관련 날짜
마지막으로 수정한 날짜 2022-03-28 오후 5:52
만든 날짜 2021-08-31 오전 1:55
마지막으로 인쇄한 날짜

관련 사용자
만든 이 Administrator
만든 이 추가
마지막으로 수정한 사람 Acer

Figure 2. File properties of Donation receipt (OOO).doc

Although the attack method and the file's features are the same as described in the previous blog, this attack creates a batch file with a different name when the macro is run. The batch file was distributed as moster.bat, and its features are identical to those of "error.bat" in the previous blog.

- C:\Users\Public\Documents\moster.bat -> Register start.vbs file to RUN key, run no4.bat file, and download additional files
- hxxp://nomonth-man.com/dfg04/%COMPUTERNAME%.txt (Additional file download URL)

It appears that the attacker is currently attempting to expand their scope of attack beyond North Korea professionals and virtual asset professionals. Users must be cautious when downloading attachments from emails or websites of unknown sources. When running Word files, extra caution is needed if there are messages or images that prompt the users to click Enable macro as clicking it may run a malicious macro.

AhnLab's anti-malware software, V3, detects and blocks files related to the attack using the aliases below.

[IOC] [MD5] – no1.bat : a0fddb12d7b3c445fdb7ab602a5bf5fb – download.vbs : 85165e07b9f198a5e4047756eb779b46 – temp.doc : f248401769bbcd0ebeff992ef3cfe678 – moster.bat : 07232fe7144b0286eb5c9882834eea96 – no4.bat : 0b41f93365ec443406df942914317ec7 – start.vbs : 050e663bf6c97a953e25eb7e9754d656 – upload.vbs : a40eaa73ccffe4bc2233bdfd84fe2d62

[Detection Name (Engine ver.)] – no1.bat : Trojan/BAT.Runner (2022.03.30.00) – download.vbs : Downloader/VBS.Generic (2022.03.30.00) – temp.doc : Trojan/DOC.Agent (2022.03.30.01) – moster.bat : Trojan/VBS.Akdoor (2022.03.30.00) – no4.bat : Trojan/VBS.Akdoor (2022.03.30.00) – start.vbs : Trojan/VBS.Runner (2022.03.30.00) – upload.vbs : Trojan/VBS.Akdoor (2022.03.30.00)

[C&C] – hxxp://nomonth-man.com/uio04/upload.php

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

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

Categories:Malware Information

Tagged as:APT, Kimsuky