Appleseed Being Distributed to Nuclear Power Plant-Related Companies - ASEC

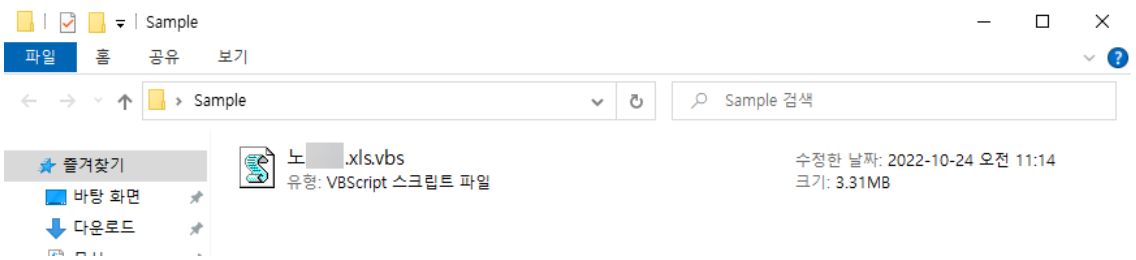
By ATCP

Published: 2022-10-26 · Archived: 2026-04-05 16:03:21 UTC

The ASEC analysis team has recently discovered a case of AppleSeed being distributed to nuclear power plant-related companies. AppleSeed is a backdoor malware used by Kimsuky, one of the organizations affiliated with North Korea, and this malware is being actively distributed to many companies.

The filenames of the AppleSeed dropper were identified by the ASEC analysis team as follows, and a double file extension was used to deceive users.

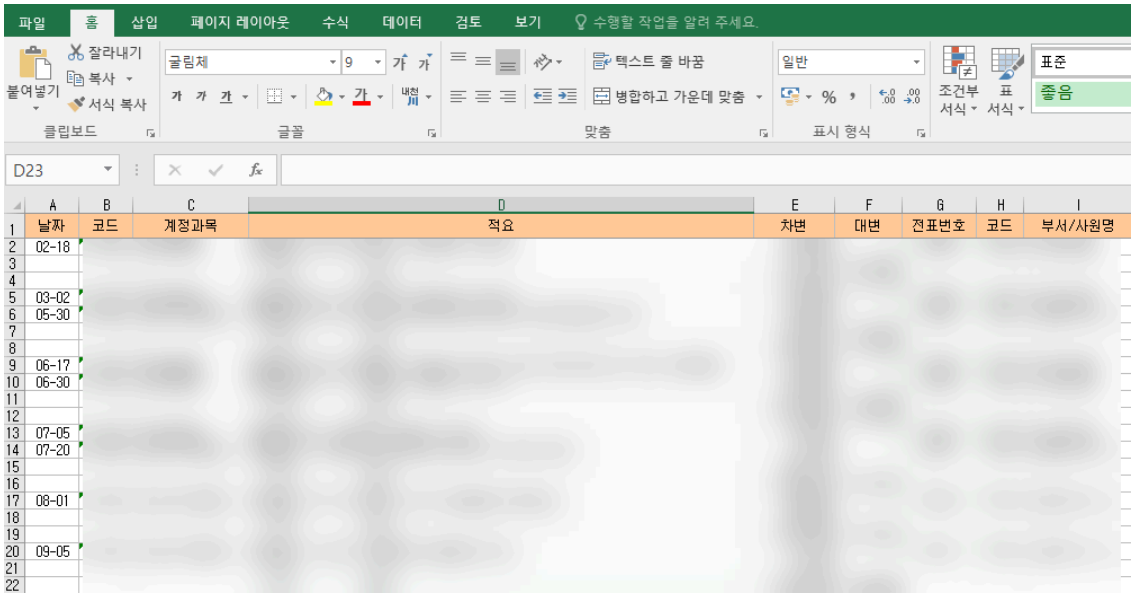
- **노**.xls.vbs (Noh**.xls.vbs)**
- **배치도_고리2호기ISI.pdf.vbs (Layout_KoriNo2ISI.pdf.vbs)**



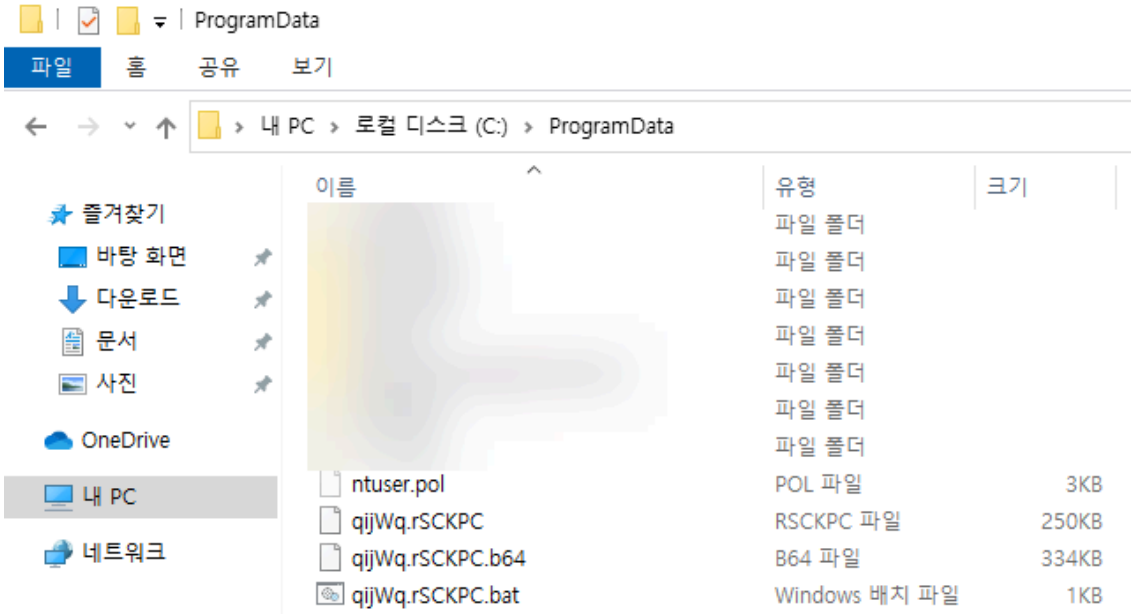
When the file is executed, the encoded data inside is decoded and each file is created in the paths below.

- **[The same path as the vbs file]\Noh**.xls (Normal Excel bait file)**
- **%ProgramData%\qijWq.rSCKPC.b64 (Malicious PE file encoded in a certain format)**
- **%ProgramData%\qijWq.rSCKPC.bat (Batch file that decodes the qijWq.rSCKPC.b64 file)**

The printed Excel file is automatically opened, making it seem as if the user has opened a normal Excel document. The Excel bait file contains texts related to nuclear power plants (See Figure 2).



In the background, the qijWq.rSCKPC**.bat** file in the %ProgramData% path is executed, which decodes qijWq.rSCKPC**.b64**, ultimately creating the qijWq.rSCKPC file (DLL PE).



Afterward, the dropped malware is executed via regsvr32, a program that executes DLL files. The exact execution argument is as follows.

- **regsvr32 /s /i:123579ASDFG C:\ProgramData\qijWq.rSCKPC**

After the file is executed, the malware accesses the C2 below to receive and carry out the commands. Then, it encodes the results in a certain format to transmit to C2.

- **C2 : hxxp://ndt.info[.]gf/index.php**
- **Commands**
  - die: Terminate
  - getinfo: PC information
  - where: Currently running path
  - run: Executes certain files or commands

```
1  getinfo
2  Host Name :
3  User Name :
4  OS Name : Windows 10 Pro 20H2(OS Build .746)
5  OS Arch : x64
6  Engine Arch : x64
7  Vaccine Info : Windows Defender
```

The attacker can use the run command to execute desired behaviors, as well as download and execute additional malware files such as AppleSeed.

Because the bait file is also run, users normally cannot recognize that their systems are infected by malware. As the files mentioned above mainly target certain companies, users should refrain from running attachments in emails sent from unknown sources.

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

[File Detection]
Dropper/VBS.Generic.SC183898
Dropper/Win.AppleSeed.R531012
Dropper/VBS.VBS

MD5

55a9a935b36da90fb5a7ab814d567a40

ba83312ea92c284c710bcc0906a29fb1

Additional IOCs are available on AhnLab TIP.

URL

http[:]//ndt[.]info[.]gf/index[.]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/41015/