

Distributing AppleSeed disguised as Internet router installation file

The ASEC analysis team caught the situation where the AppleSeed malware was disguised as a router firmware installer on May 26th. AppleSeed, known so far, was mainly distributed under the guise of normal document files or picture files. The dropper malware that creates AppleSeed uses a script format such as JS (Java Script) and VBS (Visual Basic Script), or even an executable file has a pif extension disguised as a document file. Disguised icons and file names were used.



[Figure 1] Icon disguised as router firmware installation file

- File name: firmware upgrade installer.exe



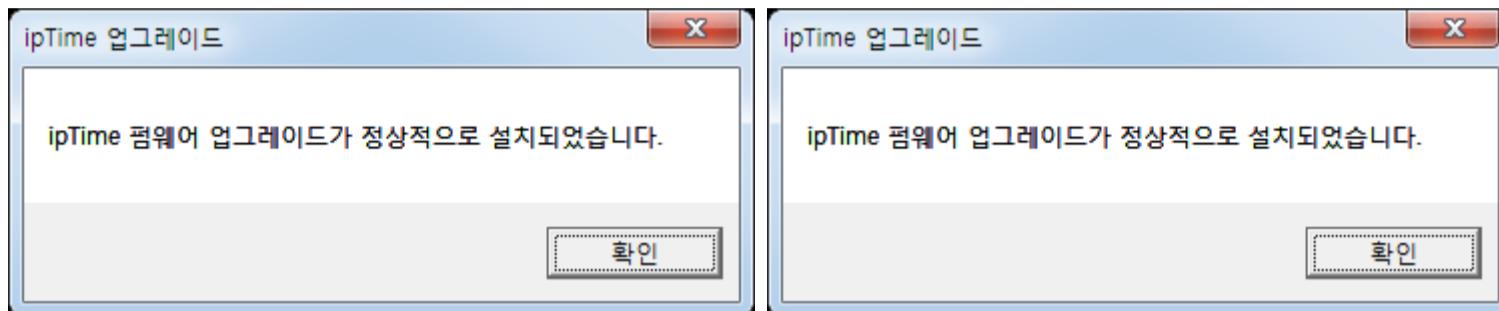
VBS scripts disguised as

PDF documents (Kimsuky) — ASEC BLOG The ASEC analysis team confirmed today (03/23) that the attack group presumed to be the Kimsuky organization is performing APT attacks on specific domestic companies. When the VBS extension script file is executed, the normal PDF file existing inside is executed to deceive as if reading a normal document, and information leakage function is performed through the malicious DLL file. When

looking at the contents of the PDF document, the attack target is estimated to be a precision processing company, and the contents of the PDF document are as follows. File name: Receipt - Small and Medium Business Technology Innovation Development Project_Market Expansion_Green Conversion_S?????.pdf.vbs...

As for how the EXE executable file works, when the user runs the file, a pop-up window disguised as the firmware upgrade installation of a specific router occurs as shown below. (It has nothing to do with the router firmware and AppleSeed malware.) For reference, in the case of disguised document files in the past, the documents and picture files are popped up when executed, disguised to appear as if the user executed the document or picture normally.

If you click the OK button in the pop-up window, the EXE internally transmits “iptime.com” to the “ShellExecuteExW” API as an API parameter, so that it looks as if the firmware update is in progress normally and accessing the manufacturer’s website.



[Figure 2] Pop-up window for firmware upgrade of a specific router

웹 사이트 접속과 동시에 사용자 PC의 백그라운드에서는 AppleSeed 악성코드가 설치된다. AppleSeed는 백도어 악성코드로서 C&C로부터 명령을 받아 정보 탈취 및 추가 악성코드 생성 등 다양한 악성 행위를 수행할 수 있다. 현재까지 유사한 사례를 분석한 결과 공격자는 타겟 PC에 주로 원격 제어를 위한 RDP Patcher, HVNC, TightVNC 및 메타스플로잇 미터프리터를 추가로 설치하였다.

AppleSeed는 다음과 같이 정상 프로그램을 위장한 경로에서 동작하며, 자사 ASD 로그 확인 결과 공격자는 또 다른 AppleSeed를 추가적으로 설치하는 것이 확인되었다.

- AppleSeed 설치 경로 (1) : %ALLUSERSPROFILE%\Firmware\Microsoft\Windows\Defender\AutoUpdate.dll
- AppleSeed 설치 경로 (2) : %ALLUSERSPROFILE%\Software\ControlSet\ServiceScheduler.dll

참고로 최근 확인되고 있는 AppleSeed는 Anti Sandbox 기능이 포함되어 있는데, DllInstall() 함수에 악성 루틴이 포함되어 있어 /s 옵션 외에도 다음과 같이 /i 옵션을 통해 추가적인 인자를 받아 매칭되어야 정상적으로 동작할 수 있다.

- AppleSeed 동작 방식 및 커맨드라인 옵션 (1) : regsvr32.exe /s C:\ProgramData\Firmware\Microsoft\Windows\Defender\AutoUpdate.dll
- AppleSeed 동작 방식 및 커맨드라인 옵션 (2) : regsvr32.exe /s /n /i:123qweASDTYU C:\ProgramData\Software\ControlSet\ServiceScheduler.dll

AppleSeed 악성코드는 Kimsuky 조직의 APT 공격에 주로 사용되는 백도어 악성코드로서 다음 ASEC 블로그를 통해 상세한 분석 보고서를 소개한 바 있다.



Kimsuky 그룹의 APT 공격

분석 보고서 (AppleSeed, PebbleDash) – ASEC BLOG 본 문서는 최근 Kimsuky 그룹에서 사용하는 악성코드들에 대한 분석 보고서이다. Kimsuky 그룹은 주로 스피어피싱과 같은 사회공학적 공격 방식을 이용하는데, 첨부 파일들의 이름으로 추정했을 때 공격 대상들은 주로 북한 및 외교 관련 업무를 수행하는 사용자들로 보인다. 자사 ASD 인프라의 감염 로그를 보면 공격 대상은 일반적인 기업들보다는 개인 사용자들이 다수인 것으로 확인되지만, 공공기관이나 기업들 또한 지속적으로 공격 대상이 되고 있다. 대표적으로 국내 대학교들이 주요 공격 대상이며 이외에도 IT 및 정보통신업체, 건...

대체로 해당 악성코드는 단독으로 유포되지 않고, 사용자가 악성코드에 감염되었다는 사실을 인지하지 못하도록 미끼 문서가 함께 실행되도록 유포된다. 최초 유포는 주로 스피어 피싱 메일을 통해 이루어지므로 출처가 불분명한 사용자의 첨부 파일은 되도록 열지 않도록 주의가 필요하다.

[IOC] MD5 (1) firmware upgrade installer.exe (39b39ca9cbf9b271590d06dfc68a68b7) – Dropper/Win.AppleSeed.C5150014 (2022.05.30.02) (2) firmware upgrade installer.exe (851e33373114fef45d0fe28c6934fa73) – Dropper/Win.AppleSeed.C5145023 (2022.05.27.02) (3) wmi-ui-99bbc08f.db (9ac572bdca96a833a40edcaa91e04c2b) – Backdoor/Win.AppleSeed.C5145022 (2022.05.30.02) (4) asd.dat (6b10482c939fc33c3a45a17f021df32b), ServiceScheduler.dll (c99f6d1c7c0d55ce1453dd08c87ee2b4) – Backdoor/Win.AppleSeed.C5145020 (2022.05.27.02)

C&C – hxxp://fedra.p-e[.]kr// – hxxp://printware2.000webhostapp[.]com// – hxxp://leomin.dothome[.]co.kr/update/?mode=login

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 ‘AhnLab TIP’ 구독 서비스를 통해 확인 가능하다.

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

Categories: [Malware information](#)

Tagged as: [AppleSeed](#) , [Kimsuky](#)