3. 감염 은닉 형 악성코드 분석

1. 개 요

최근 은폐기능이 구현된 악성코드가 많이 출현하고 있다. 이러한 은폐기능은 악성코드 파일 및 프로세스 등을 은닉시켜 사용자가 감염사실을 인지하지 못하게 하므로써 악성코드의 생존력을 높인다. 이번에 확인된 사례의 경우, 악성코드 제작자는 백도어 기능 등이 구현된 악성코드를 설치한 후, 해당 악성코드들을 은폐하기 위하여 은폐를 위한 전용 악성코드(iistart.exe)를 추가로 설치하였다. 은폐를 목적으로 제작된 악성코드는 프로세스 은닉, 네트워크 접속 은닉, 악성파일 은닉 등의 기능을 수행하며, 은닉 대상은 임의로 설정, 변경이 가능하도록 구현되어 있었다. 악성 프로세스 및 파일, 악성 네트워크 접속이 은닉될 경우, 감염인지가 늦어져, 조기 대응에 어려움이 발생할 수 있다.

최근에 이러한 은닉형 악성코드가 많이 출현하고 있으므로, 감염이 의심되는 PC 분석 시에 악성 프로세스 및 파일 등이 직접 확인되지 않는다고 하여 감염되지 않은 것으로 섣불리 단정하지 않도록 주의하여야 한다.
또한, 백신을 업데이트하여 주기적으로 점검하고, 윈도우 OS 및 MS Office 와 Adobe 등 자주 사용하는 Third-Party 제품군에 대한 최신 패치를 실시하여 감염을 사전에 예방할 필요가 있다.

2. 감염 및 은닉 방법

■ 은닉 방식

공격자는 은닉전용 악성코드인 iistart.exe를 통하여 이미 감염되어 있는 다른 백도어 악성코드들을 은폐하였다. 은닉대상은 iistart.inf 파일에 정의되어 있었다.

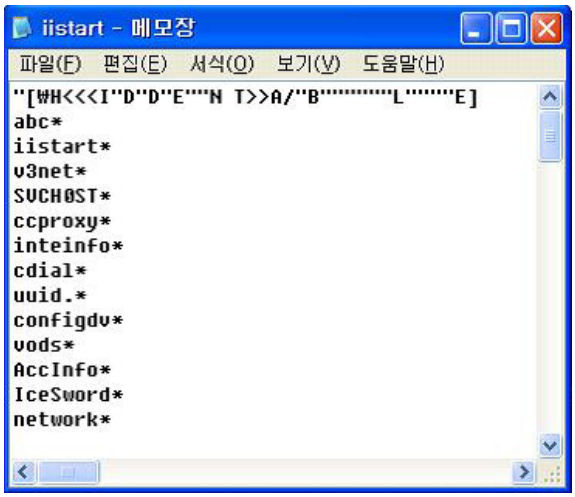
■ 은닉기능이 구현된 악성코드 iistart.exe 분석

iistart.exe는 다른 악성코드를 은닉시키기 위한 코드이다. 공격자는 iistart.inf 설정파일을 통하여 아래와 같이 은닉대상을 정의하였다.

- 은폐기능 상세

▶ 파일 은닉 예

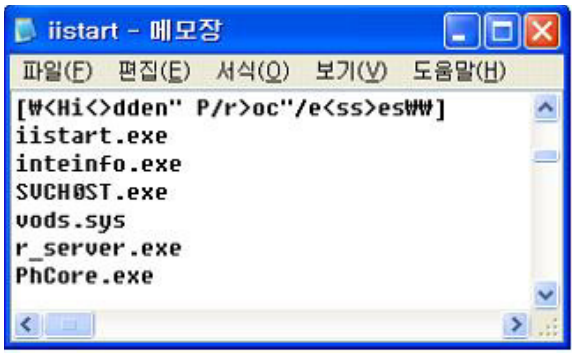
iistart.inf파일에 오른쪽 같이 은폐를 원하는 파일 및 폴더 문자열을 정의한다. 해당 문자열을 가지는 파일 및 폴더는 은닉되는 것으로 확인되었다.



〈은닉 대상 폴더 및 파일 예 (iistart.inf)〉

▶ 프로세스 은닉 예

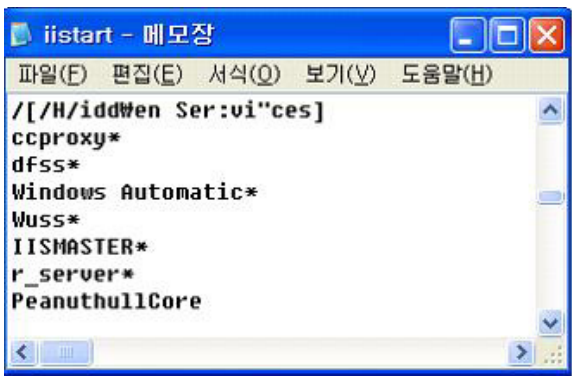
iistart.inf에 은닉시키고자 하는 프로세스를 정의할 수 있다. 오른쪽 예는 실제 공격자가 은닉을 위하여 정의해 놓은 내용이다



〈은닉 대상 프로세스 정의 예 (iistart.inf)〉

▶ 윈도우 서비스 은닉 예

iistart.inf에 아래와 같은 정의를 통하여 서비스를 은닉시킬수 있다. 문자열이 포함되어 있는 서비스는 은닉된다.



〈은닉 대상 서비스 정의 예 (iistart.inf)〉

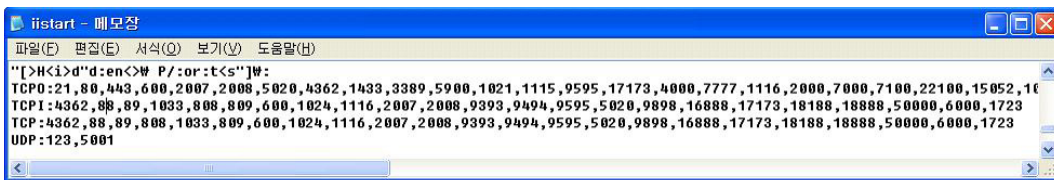
▶ 레지스트리 키 값 은닉 예

iistart.inf에 정의되어 있는 옆의 이름의 키 값은 은닉된다.

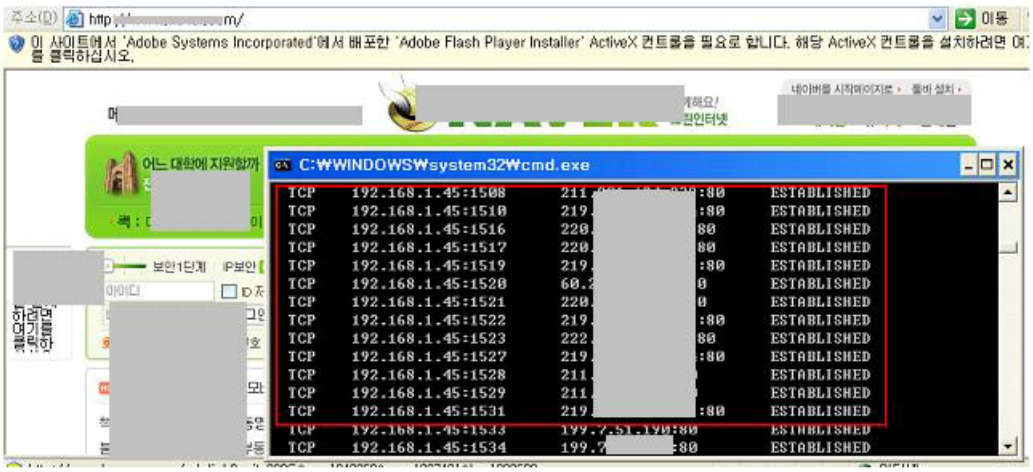
〈은닉 대상 레지스트리 정의 예 (iistart.inf)〉

▶ 네트워크 접속 은닉 예

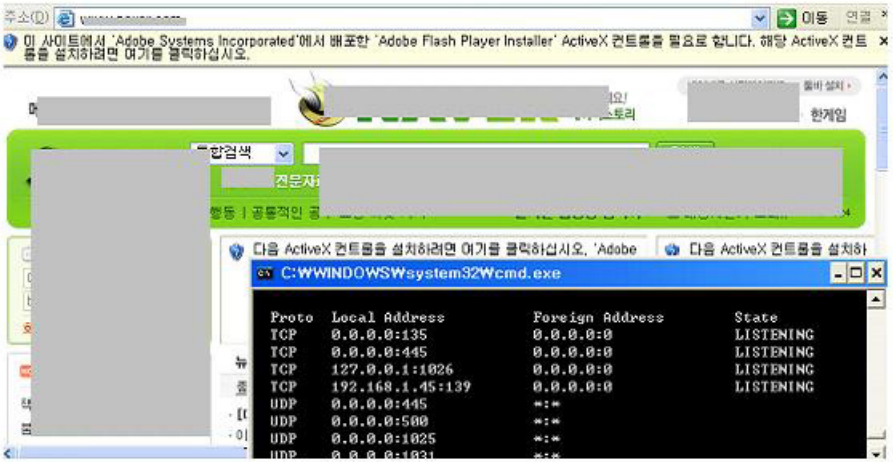
iistart.inf 에 정의되어 있는 아래의 네트워크 포트를 통한 통신은 은닉된다.



〈은닉 대상 포트 예 (iistart.inf)〉

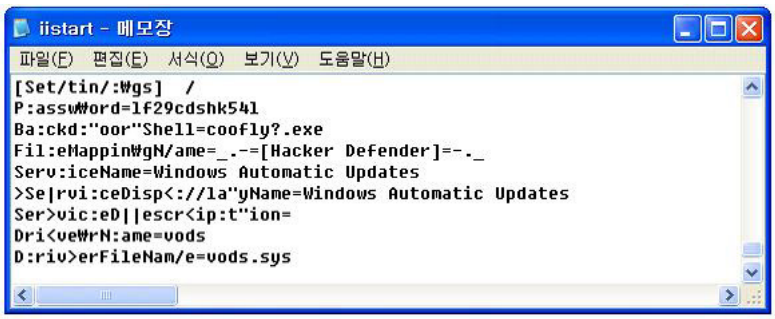


〈감염 전 TCP 80 세션 연결 예〉

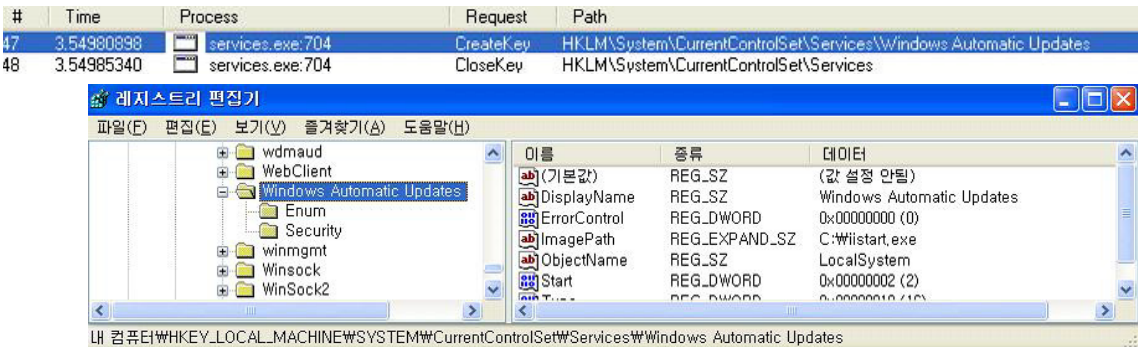


〈감염 후 TCP 80 세션 은닉 예〉

또한, iistart.exe 는 iistart.inf 에 정의되어 있는 설정값을 참조하여 활동한다.
ex) 백도어 쉘을 정의 또는 재 부팅 시 계속적으로 활동하기 위하여 서비스에 등록 등



〈재 부팅 시 계속적인 활동을 위한 윈도우 서비스 등록 예〉



은닉 대상 악성코드

감염 PC에서는 휴피곤 계열의 악성코드(SVCH0ST.exe, '0' 은 숫자 0임)가 추가로 발견되었으며, 공격자는 iistart.exe를 통하여 해당 악성코드를 은닉시켰다.
은닉의 대상이 되었던 SVCH0ST.EXE는 휴피곤 계열의 악성코드이다. 휴피곤 악성코드의 경우 감염PC를 원격에서 통제할 수 있으며, 파일유출, 키로깅 등 강력한 백도어 기능을 제공한다.

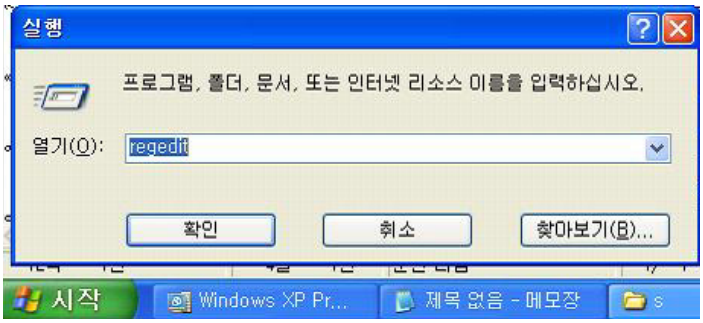
3. 결 론

PC내에 악성코드가 은닉된 형태로 감염되어 있을 경우, 감염 여부를 파악하기가 쉽지 않다. 공격자는 휴피곤 악성코드를 통하여 감염PC를 통제 및 정보를 유출하였으며, 이 휴피곤 악성코드가 오랜 기간동안 생존할 수 있도록 하기 위하여 iistart.exe 은닉 전용코드를 악용하였다.
이번에 발견된 은닉 악성코드의 경우는 확인 및 치료가 용이하였으나, 보다 치료가 어려운 커널 후킹을 통한 은닉유형도 많이 발견되고 있어 각별히 주의할 필요가 있다. 사용자는 윈도우, 오피스, 자주 사용하는 Third-Party 제품군에 대한 패치를 최신으로 적용하여, 사전 감염을 예방하도록 한다.

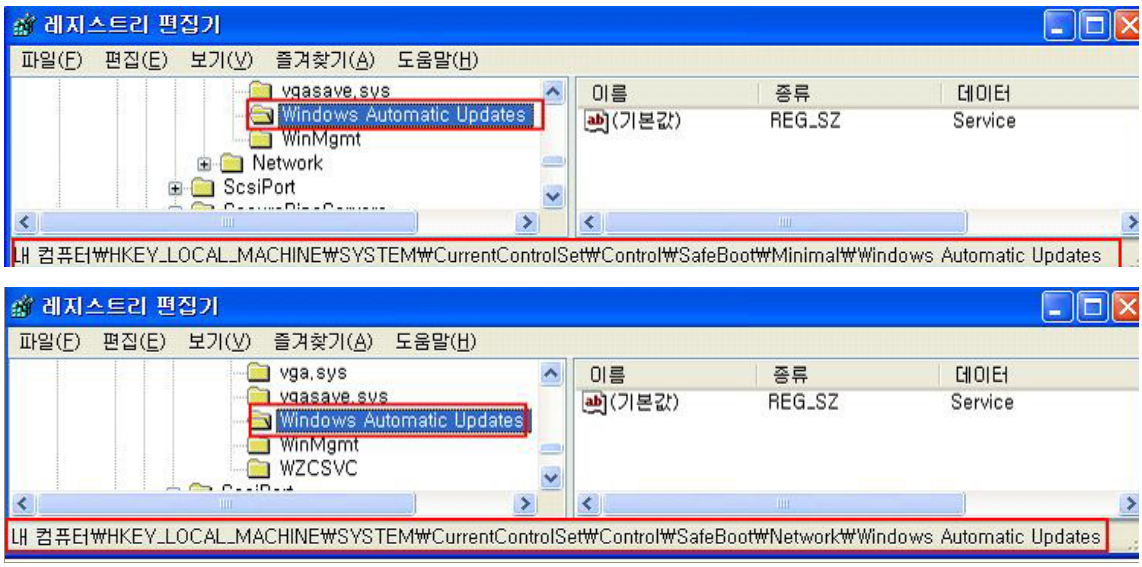
◈ iistart.exe 감염 여부 확인 및 치료 방법

■ 감염여부 확인 방법

① regedit 를 실행한다.
"시작" → "실행" → "regedit" 입력

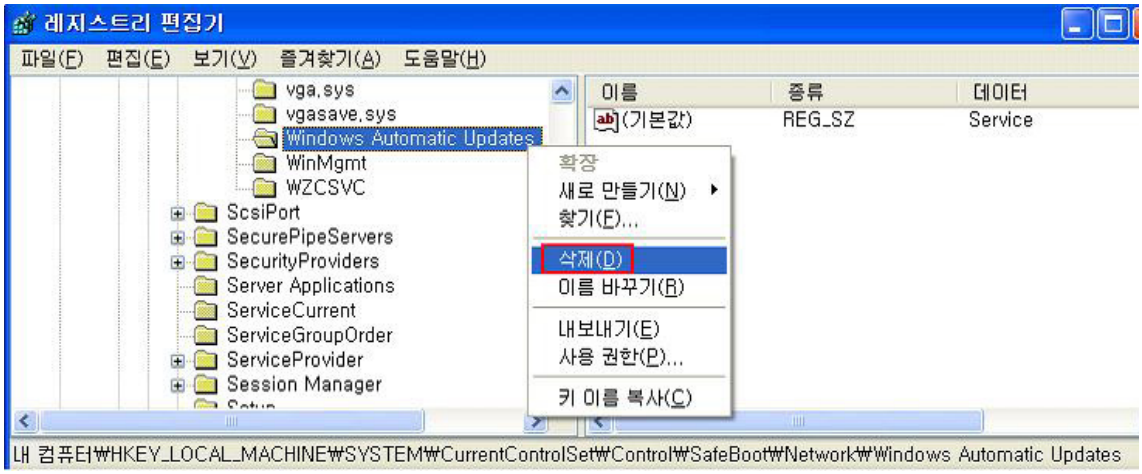


② HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal와
HKLM\SYSTEM\CurrentControlSet \Control\SafeBoot\Network에
"Windows Automatic Updated" 폴더가 존재하는지 확인한다.
아래와 같이 해당 폴더가 존재하면, 감염된 것으로 볼 수 있다.

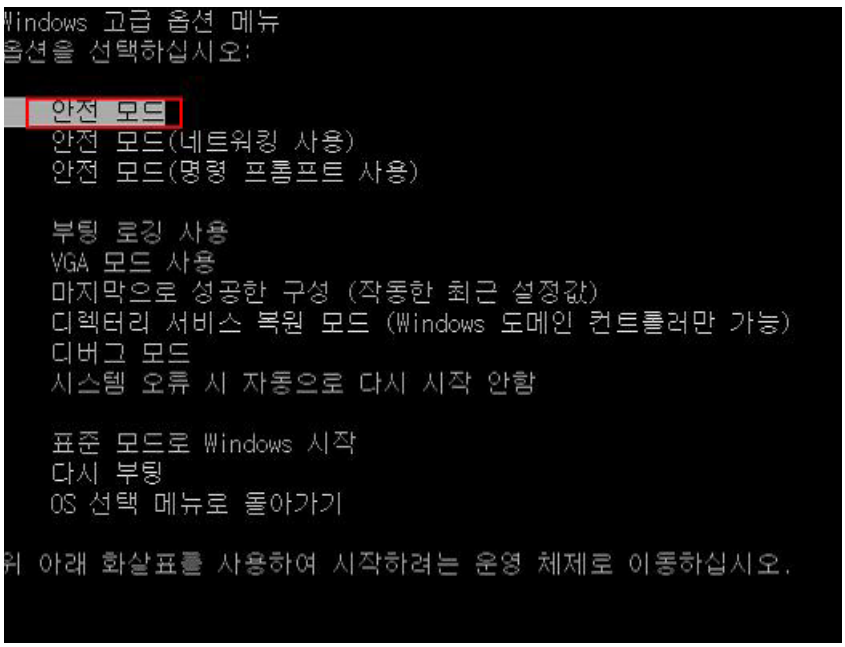


■ 치료 방법

① regedit를 이용하여
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal 와
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network의
"Windows Automatic Updated" 폴더를 삭제한다.



② 안전모드로 부팅한다. (부팅 시 F8 누른 후, 안전모드 선택)



③ 검색메뉴를 통하여 iistart.exe (64,000 byte) 파일의 위치를 찾아 해당 폴더로 이동한다.

④ iistart.exe, iistart.inf, vods.sys 파일을 삭제한다.

⑤ 재 부팅 한다.

※ iistart.exe에 감염된 PC는 iistart.exe 외에도 타 악성코드에 감염되어 있을 가능성이 높으므로, iistart.exe 치료와 함께 타 악성코드 감염여부에 대한 추가점검이 필요하다.