오픈프락시(8080/4769) 감염확인 및 제거방법

◆ 개 요

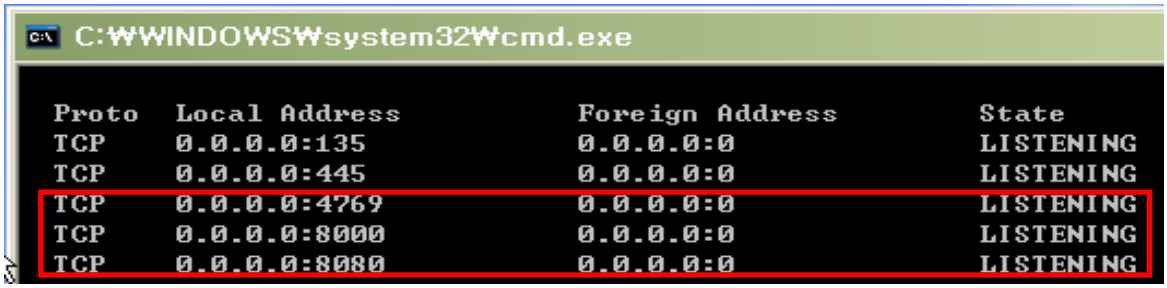
오픈프락시(8080/4769 포트)에 감염된 PC는 시스템 시작시 자동으로 해당 TCP 포트를 통해 오픈프락시 서비스를 시작하며, 주로 스팸발송에 악용되어 시스템과 네트워크의 불안정 및 속도저하를 유발합니다.

◆ 오픈프락시 감염여부 확인방법

오픈프락시는 총 4개의 파일로 구성되며, 시스템 루트(C:₩WINDOWS)에 설치되는 lass_update.exe 파일을 제외한 나머지 파일들은 자동으로 생성되는 특정 디렉토리(WINDOWS/system32/dump)에 설치됩니다. 오픈프락시 감염여부는 아래 두가지 방법 중 한가지를 통해 확인할 수 있습니다.

1. 네트워크 서비스 존재여부를 통한 확인

① 윈도우 시작 메뉴에서 '실행(R)' 선택
② "cmd" 입력 후 '확인' 선택
③ '터미널'이 나타나면, "netstat -an" 입력
④ 특정 포트(4769, 8000, 8080번)가 동시에 열려있는지 확인
: 해당 포트가 모두 "LISTENING" 상태이면 악성파일에 감염된 것임 (아래 그림의 붉은 선 표시)



2. 악성파일 존재여부를 통한 확인

① '내 컴퓨터' / '로컬 디스크(C:)' / 'WINDOWS' / 'system32'를 차례로 선택
② 'system32' 디렉토리 내에 'lsass_update.exe' 파일이 존재하는지 확인 : 존재시 감염된 것임
③ 상단의 '도구(T)' 메뉴에서 '폴더 옵션(O)' 선택
④ '보기' 탭 클릭 후 '숨김 파일 및 폴더 표시'를 선택하여 체크하고 '확인' 선택
⑤ 다시 'system32' 디렉토리 내에 'dump' 디렉토리가 존재하는지 확인: 존재시 감염된 것임

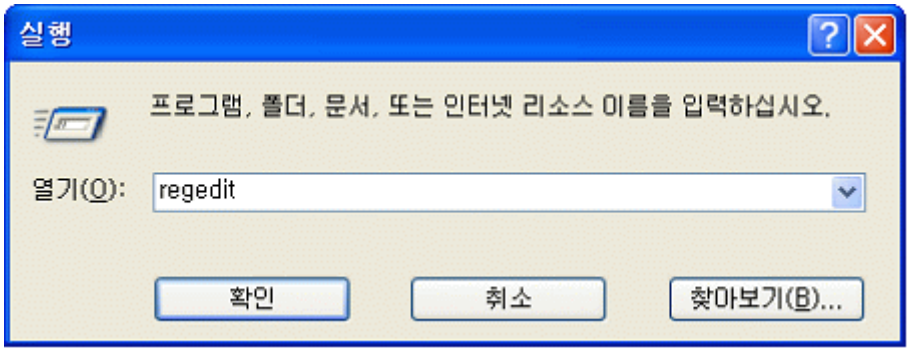
◆ 악성파일 제거방법

2006년 8월 현재 국내 주요 바이러스 백신프로그램에 8080/4769 오픈프락시가 악성프로그램으로 등록되어 있으므로, 백신프로그램을 최신으로 업데이트 하면 이를 통해 손쉽게 제거할 수 있습니다. 바이러스 백신프로그램을 사용하지 않거나 사용중인 백신프로그램이 이를 탐지하여 삭제하지 못하는 경우에는 이용자가 직접 아래 방법을 통해 제거할 수 있습니다. MS 윈도우 시스템의 경우, 프로세스가 실행되고 있을 때에는 그 이미지 파일을 제거 할 수 없으므로 시작프로그램 등록 엔트리를 삭제하고 시스템을 재시작한 후에 제거하여야 합니다.

1. 관련 레지스트리 키 제거

① 윈도우 시작 메뉴에서 '실행(R)' 선택

② "regedit" 입력 후 '확인' 클릭



③ '레지스트리 편집기'가 시작되면, 'HKEY_LOCAL_MACHINE' / 'SYSTEM' / 'CurrentControlSet' / 'Services'를 차례로 선택

④ 등록된 레지스트리 키 중에서 'ddns_update', 'lsass_update', 'proxy_update' 3개를 각각 삭제 (오른쪽 마우스 클릭 후 메뉴에서 '삭제(D)' 선택)

2. 악성파일 제거

⑤ 위 과정을 통해 3개의 레지스트리 키가 삭제되었으면, 윈도우 시스템을 재시작

⑥ '내 컴퓨터' / '로컬 디스크(C:)' / 'WINDOWS' / 'system32'를 차례로 선택

⑦ 'system32' 디렉토리 내에 있는 'lsass_update.exe' 파일과 'dump' 디렉토리 전체를 삭제

◆ 치료여부 확인

악성파일 제거 후 시스템을 재 시작 한 다음, 감염여부 확인방법 중 1번 "네트워크 서비스 존재여부를 통한 확인" 방법을 통해 특정 포트(4769, 8080, 8000번)가 "LISTENING" 상태인지 확인합니다. 해당 포트가 LISTENING 상태가 아니라면, 악성파일이 정상적으로 제거된 것입니다.