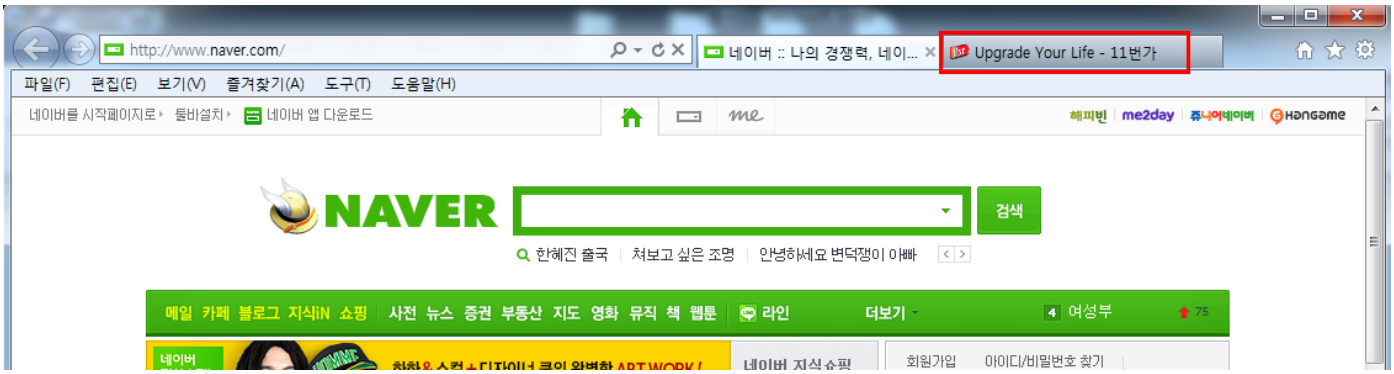
광고성프로그램 설치 사례 및 배포경로

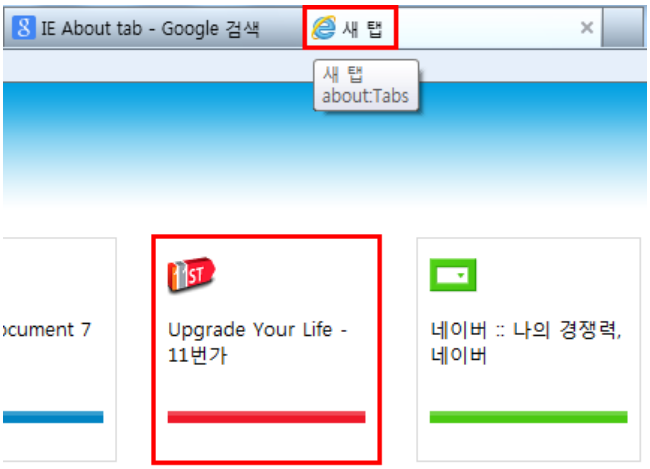
본 사례는 일례이며 , 대부분의 유사프로그램은 아래에서 소개되는 과정의 일부 , 전부 또는 추가 작업을 가지고 있을 수 있습니다.

Windowstab.exe

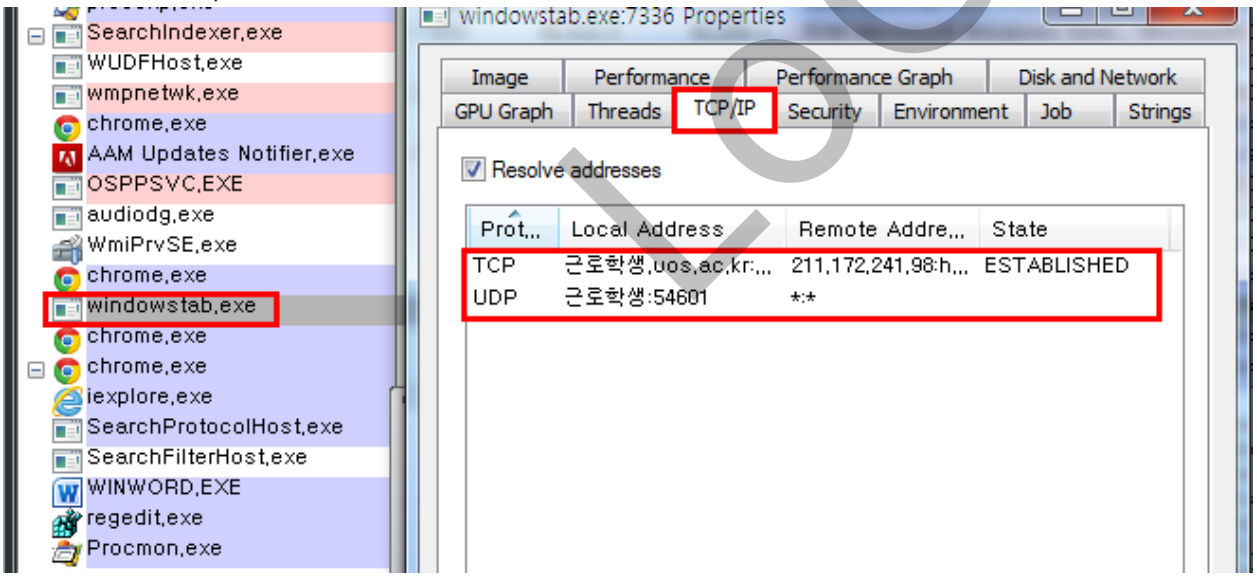
Windowstab.exe 가 실행 된 상태에서 IE 를 실행시키면 아래와 같이 광고성 탭이 하나 더 추가 된다.



또한 새 탭을 생성하여 빈 페이지에 about:Tabs 에도 목록이 추가 돼 있다.

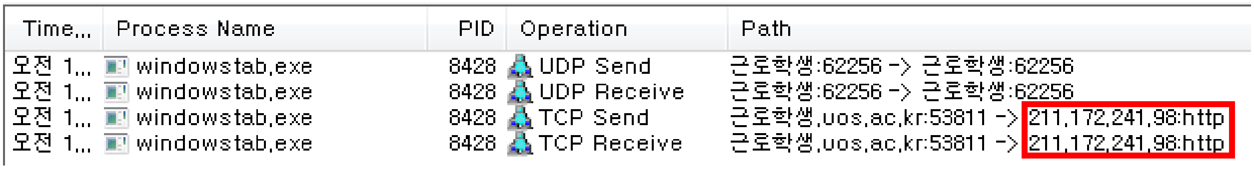


실제로 ProcessExplorer.exe 에서 해당 프로세스의 동작을 확인하고 연결된 TCP , UDP 포트를 확인했다.

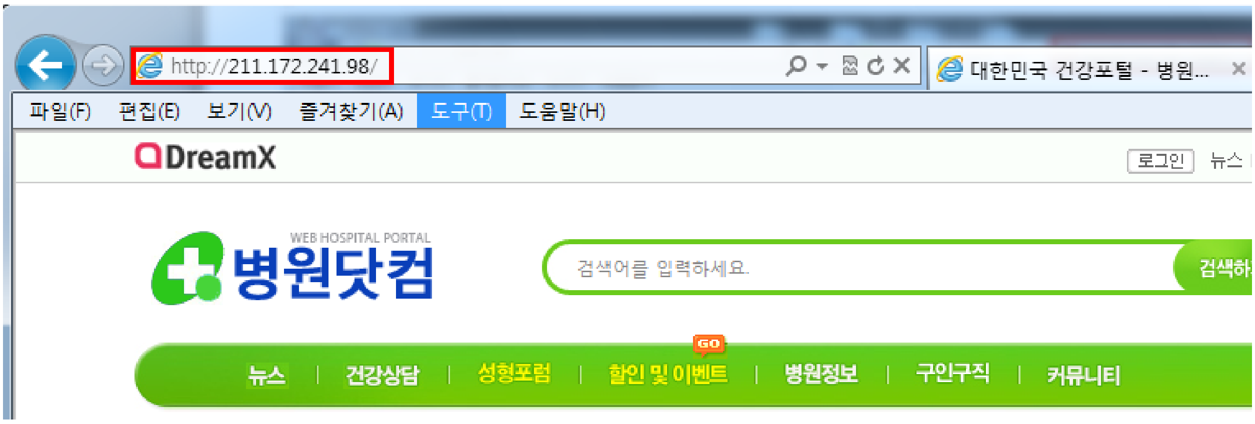


그 결과 UDP 포트는 재 실행하면 포트가 변경 되었지만 TCP 에 연결된 211.172.241.98 이라는 주소는 변경되지 않았다.

ProcessMonitor.exe 로 네트워크 동작을 살펴 본 결과도 동일하게 연결 설정이 나타난다.



아래 그림은 위 주소로 접속 했을 때 상황이다.



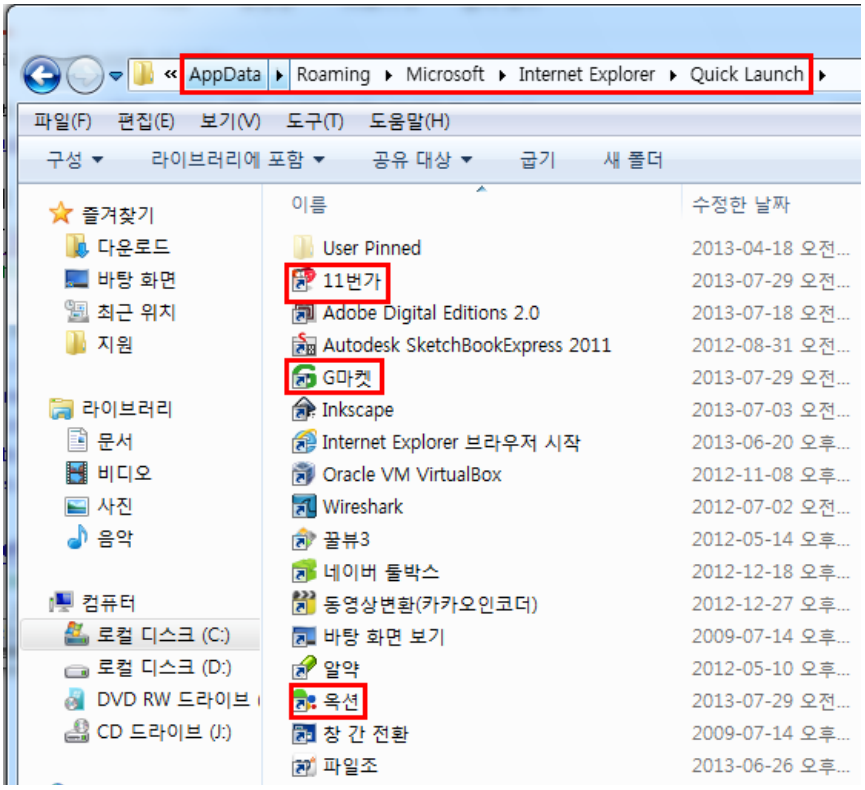
이 사이트가 windowstab.exe 가 어떤 식으로든 사용하는 주소라고 볼 수 있다.

ProcessMonitor.exe 를 통해 레지스터에 대한 행위를 본 결과 ProxyEnable 에 값을 설정하는 것이 확인 되었다.

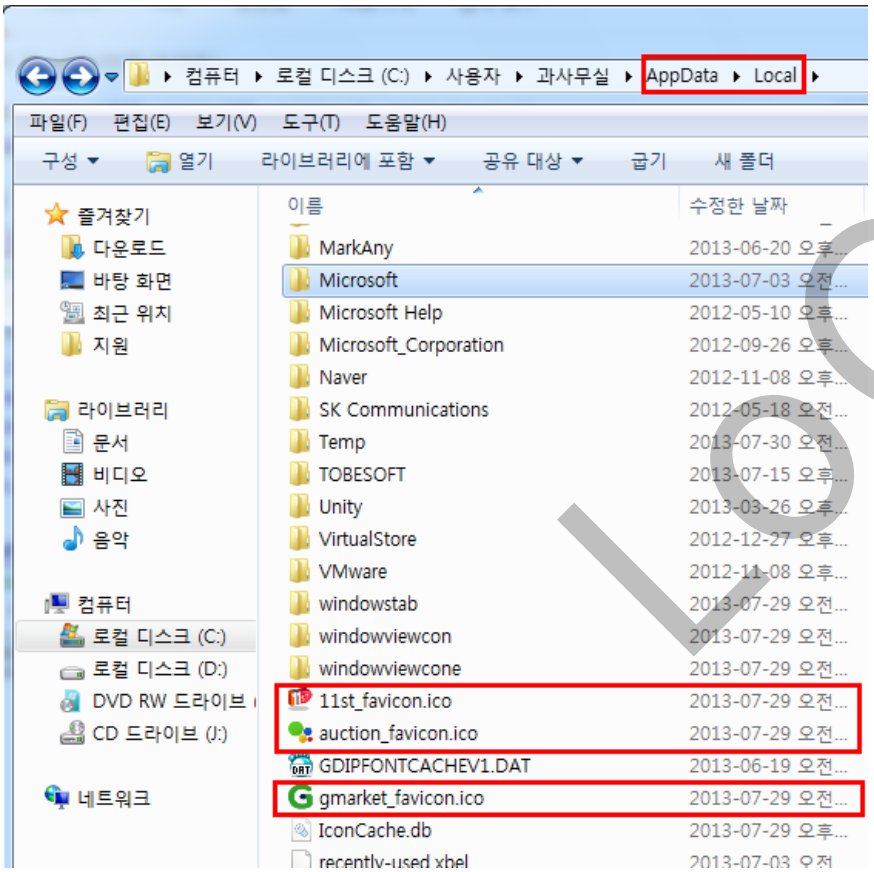
위의 주소를 경유지로 사용하고 있다고 생각 할 수 있다.

이 프로그램들과 같이 추가된 부분들을 살펴보자.

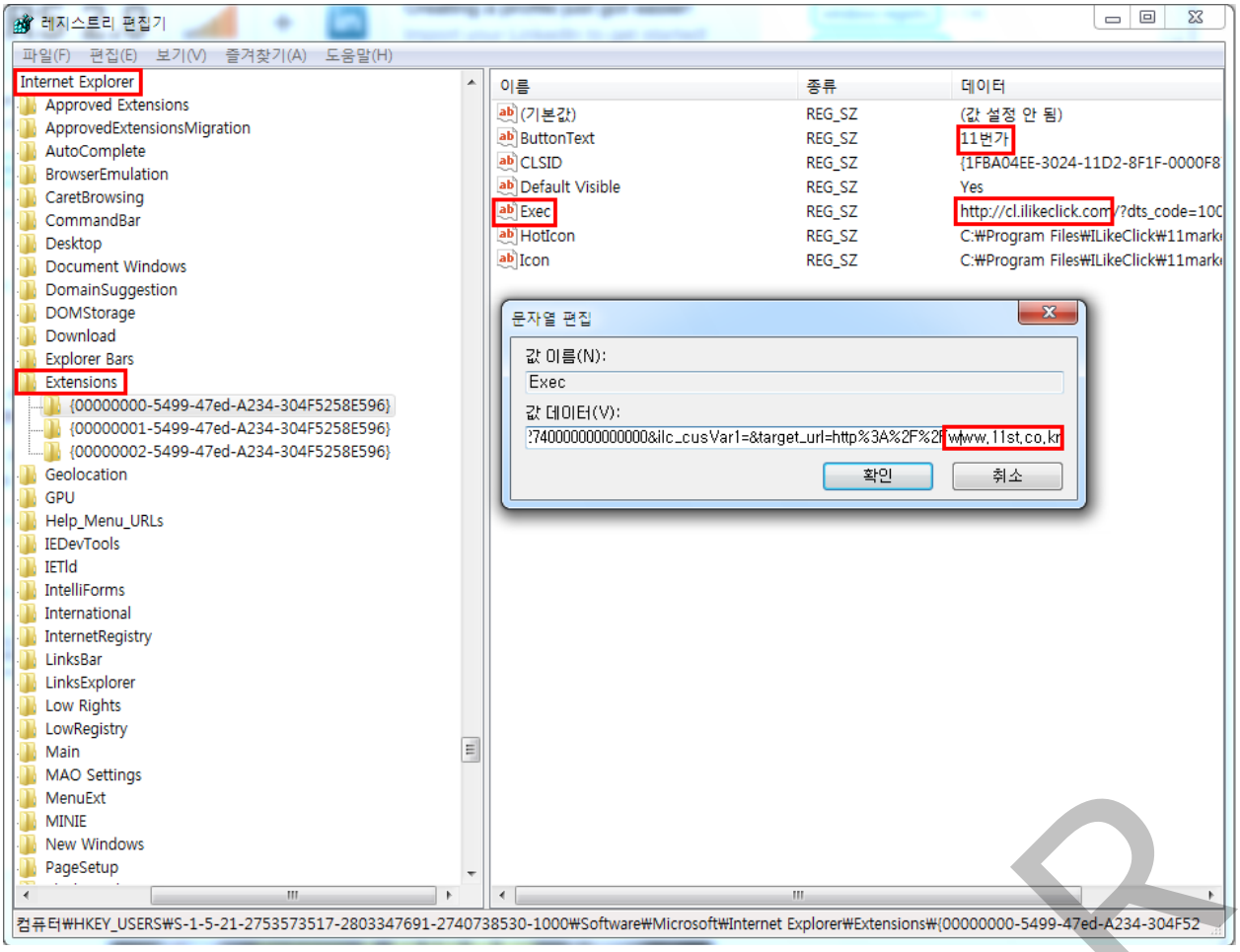
1.빠른실행 부분 에 사이트 3 개(11 번가, G 마켓, 옥션) 추가.



2.C:₩사용자₩username₩AppData₩Local₩ 에 아이콘 추가

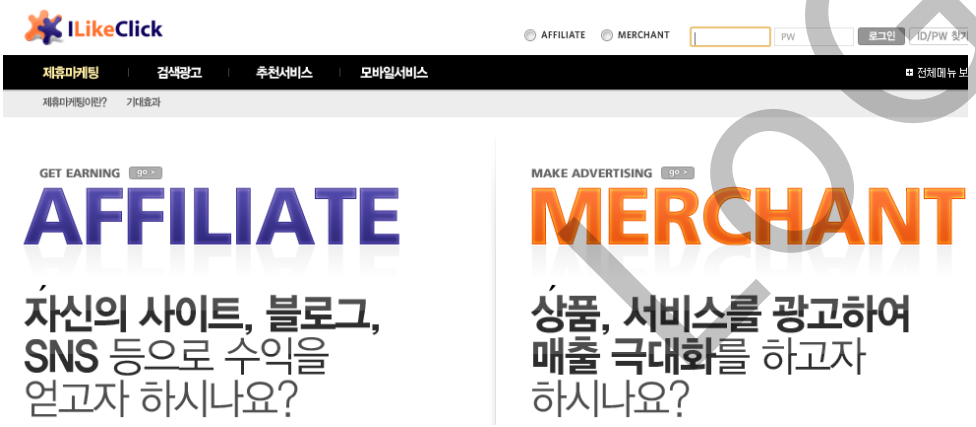


3.레지스트리 HKU₩%usersid%₩Software₩Microsoftware₩Internet Explore₩Extension 부분에 값 설정



값을 살펴보면 앞 쪽에 cl.ilikeclick.com 사이트에 주소가 있다.

아래는 실제로 cl.ilikeclick.com 을 접속한 결과이다.



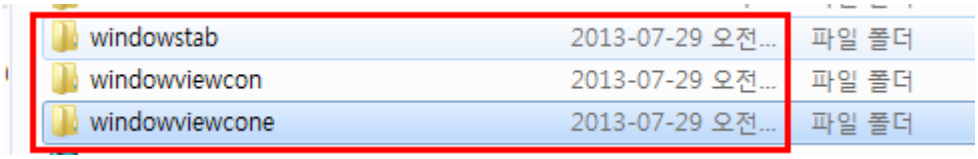
이 사이트는 제휴광고 사이트임을 알 수 있고 이 곳을 통해서 3 개의 사이트 광고가 이루어 지는 것이다.
이과 같이 제휴사이트를 통해서 광고가 이루어지기 때문에 실제로 다운 받을 경우 사용자가 눈치채지 못 하게 이미 사용자는 이러한 설치에 대한 동의를 한 것으로 여겨져 백신에서도 Adware 로 탐지하지 못 하도록 되어있다.

위에 있는 하나의 키는 11 번가에 관한 것이고
나머지 두 개는 각각 아래의 두 사이트에 대한 설정을 가지고 있다.

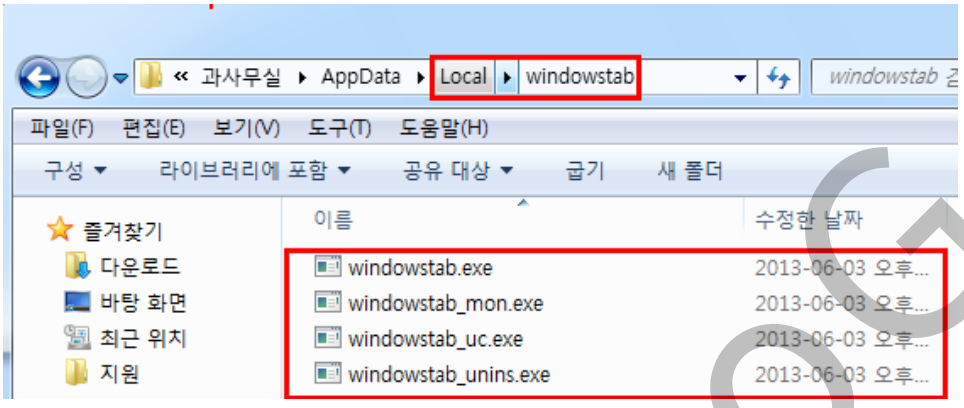
이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
ButtonText	REG_SZ	G마켓
CLSID	REG_SZ	{1FBA04EE-3024-11D2-8F1F-0000F8
Default Visible	REG_SZ	Yes
Exec	REG_SZ	http://cl.ilikeclick.com/?dts_code=10C
HotIcon	REG_SZ	C:₩Program Files₩ILikeClick₩gmarket
Icon	REG_SZ	C:₩Program Files₩ILikeClick₩gmarket

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
ButtonText	REG_SZ	옥션
CLSID	REG_SZ	{1FBA04EE-3024-11D2-8F1F-000
Default Visible	REG_SZ	Yes
Exec	REG_SZ	http://cl.ilikeclick.com/?dts_code=
HotIcon	REG_SZ	C:₩Program Files₩ILikeClick₩Auc
Icon	REG_SZ	C:₩Program Files₩ILikeClick₩Auc

4.~AppData₩Local₩ 하위에 세 개의 디렉터리 생성



아래는 각각의 디렉터리에 들어있는 내용을 보여 주고 있다.



4 개의 .exe 파일 중 windowstab_mon.exe 와 windowstab_uc.exe 는 virustotal 에서 꽤 많은 탐지율을 보이지만 메인 프로그램인 windowstab.exe 의 탐지율은 아래처럼 낮은 상황이다.

virustotal

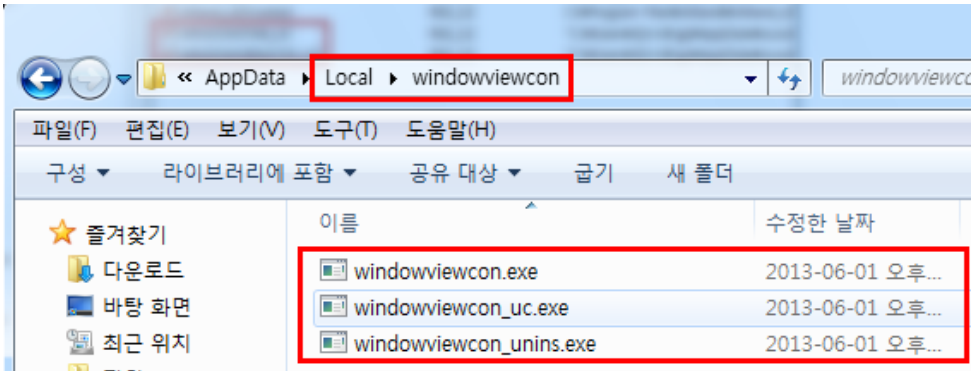
SHA256: 7539ea35301bfc3b86996cdfa4f8ab0ce16cd820ae36c49f54a20d3d60cf09f8

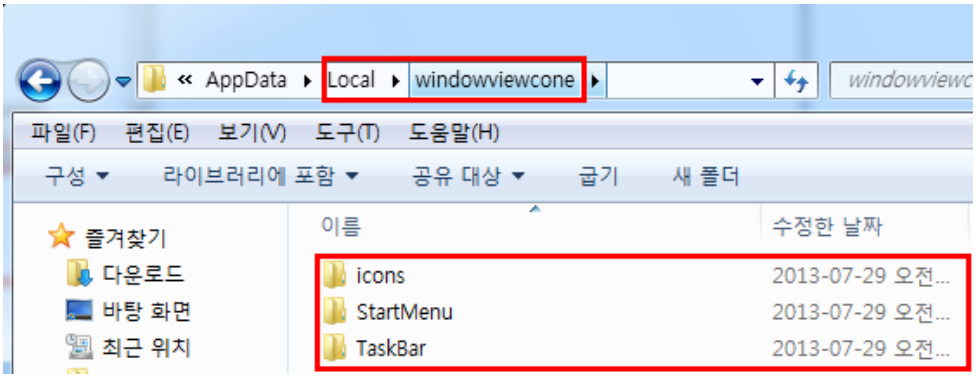
파일 이름: windowstab.exe

탐지 비율: 4 / 46

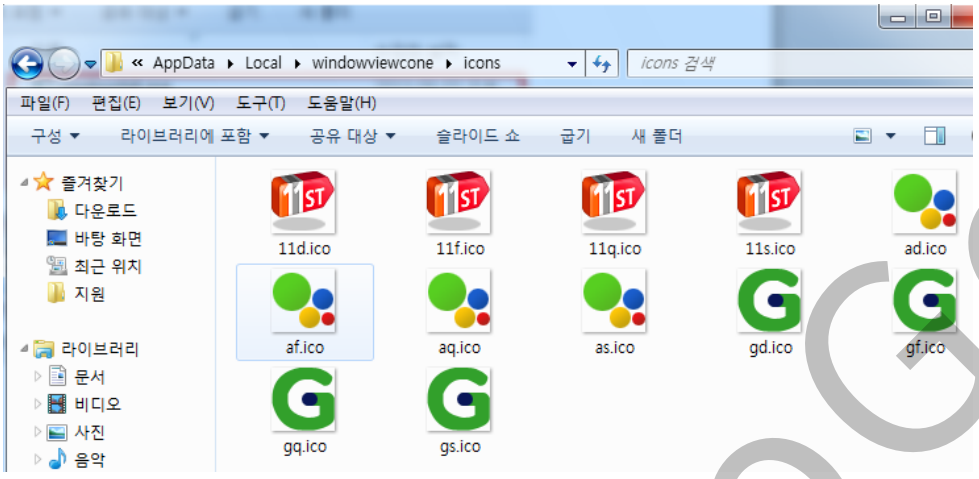
분석 날짜: 2013-07-30 04:36:57 UTC (0분 전)

실질적으로 불법이 아니기 때문에 어떤 프로그램을 다운 받을 경우 사용자가 조심하는 수 밖에 없다.
일반 사용자는 어떻게 찾아서 지워야 할지 모르기 때문에 이런 것 하나 때문에 포맷을 하거나 계속 광고에 노출 될 수 밖에 없다.

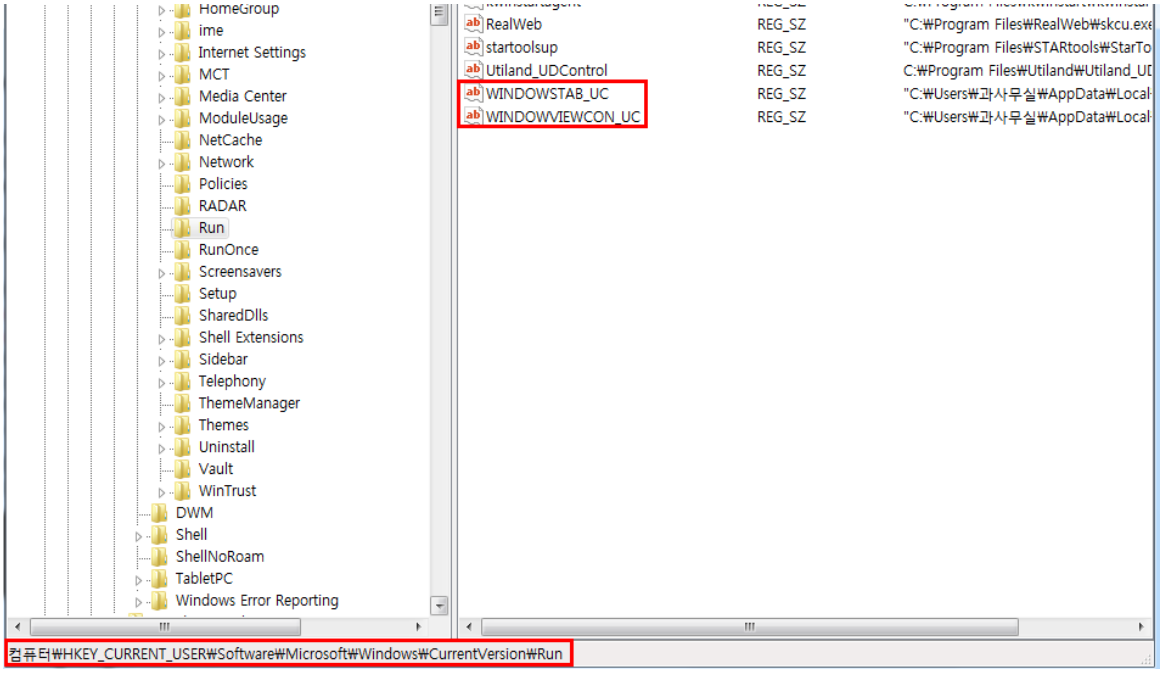




이러한 프로그램이 또 존재해서 시작메뉴나 작업표시줄에도 3 개 사이트에 대한 바로가기가 존재한다.

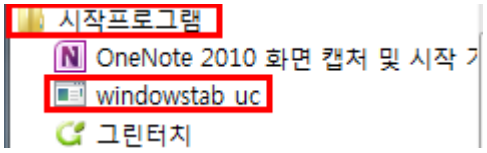


5.자동실행에 해당 프로그램 추가

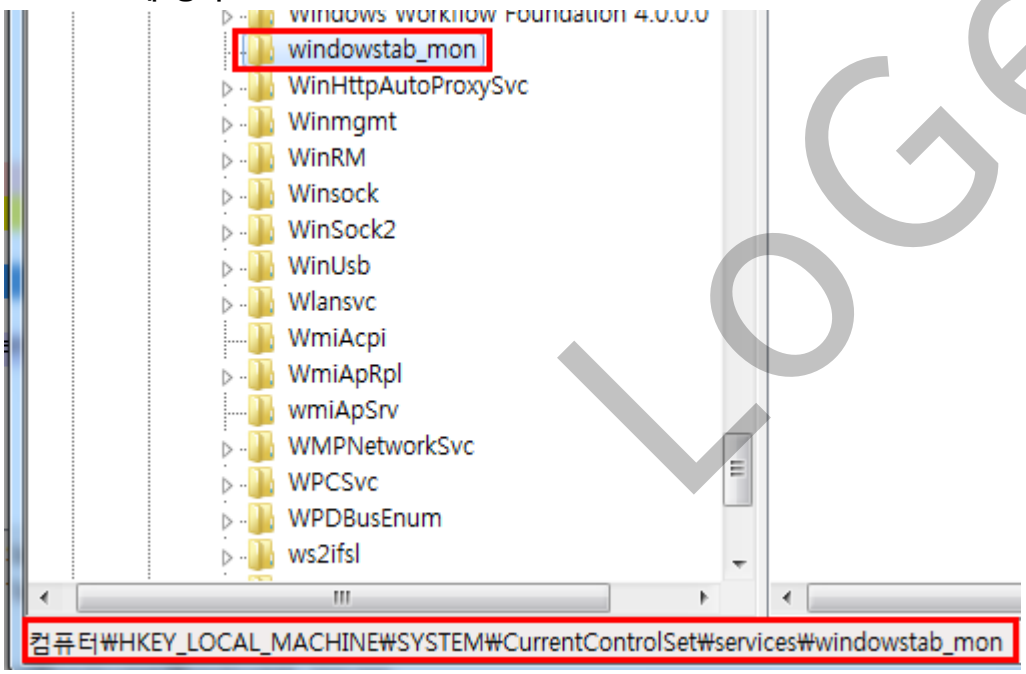


이 때문에 재부팅을해도 마찬가지로 광고 탭이 나오게된다.

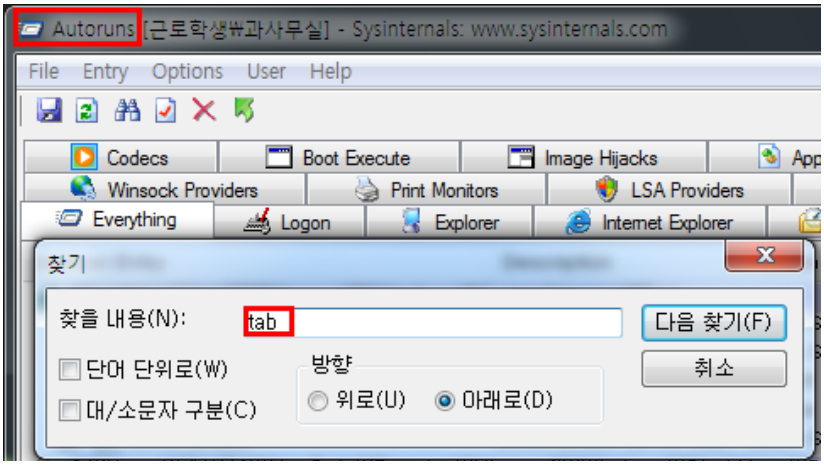
6.시작프로그램에 등록



7.services 에 등록



Autoruns 를 실행시켜 "tab" 문자열을 검색하면 해당 프로그램에 대해 설정된 자동실행 레지스트리를 찾을 수 있다.



제거방법

이러한 프로그램은 불법이 아니기 때문에 제어판->프로그램 제거 또는 변경에서 해당 프로세스를 제거할 수 있다. 또한 위에서 포함된 프로그램 중에서 ~unins.exe 를 동작시키면 제거가 가능하다.

제거 한 후 즐겨찾기나 바로가기 등이 모두 제거 됐는지를 확인하고 제거 안 된 경우가 있다면 없애주자.

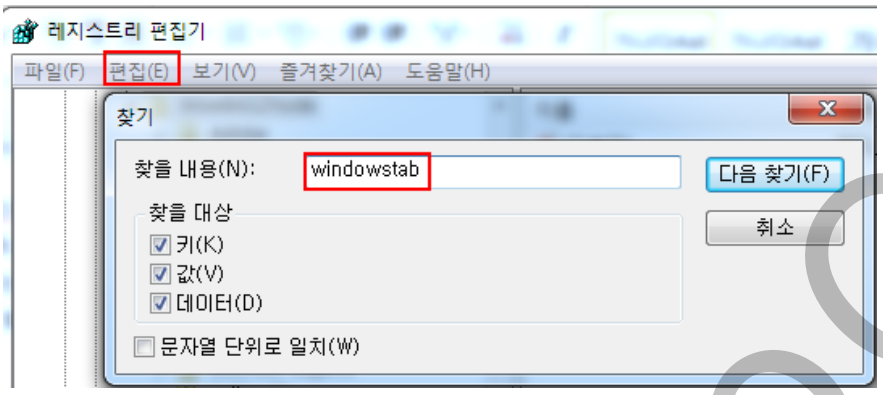
레지스트리에서 잔여 값 제거하기

프로세스를 모두 제거해도 레지스트리 키나 값은 제거하지 않는 경우가 있을 수 있다.

이 때는 백신 등에 종종 있는 레지스트리 클리너를 사용해도 되고 직접 찾아서 제거해도 된다.

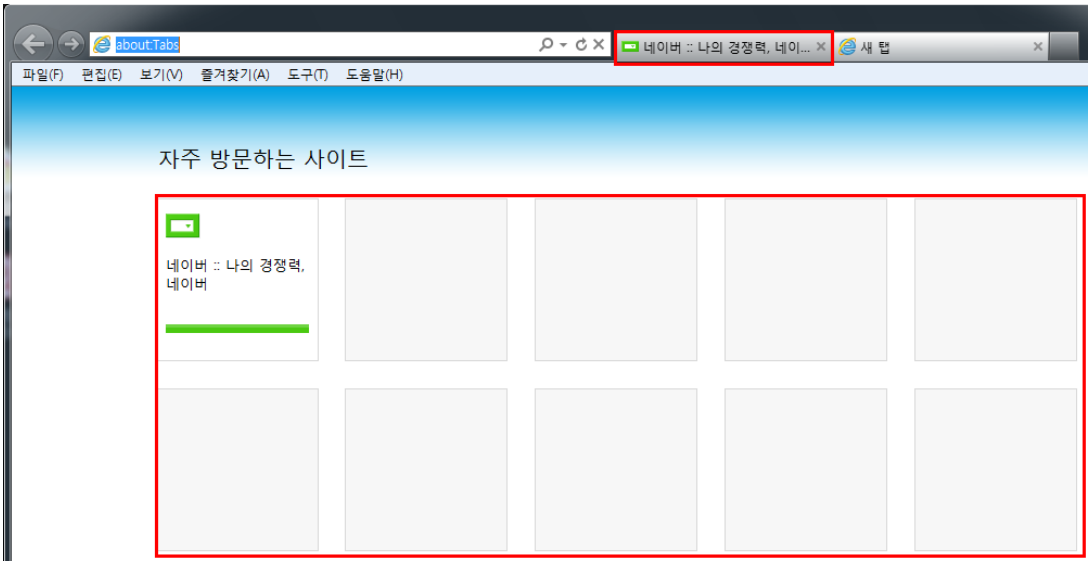
직접 찾아서 제거하는 방법은 아래와 같다

windows+R -> regedit 실행.



레지스트리편집기에서 프로세스이름을 검색해서 검색되는 값들을 제거하자. 자동실행말고도 꽤 많은 부분에 추가되어 있다. 찾을 내용에 11 번가 , 11st , G 마켓, 옥션 등을 검색하면 광고성 레지스트리 값들도 찾을 수 있다.

제거 후 재부팅해서 프로세스가 다시 시작 안 되는 것을 확인하고 IE 를 다시 시작해보자.



깨끗해 진 것을 볼 수 있다.

이러한 프로그램을 단독으로 실행시켰을 경우 프로그램 자체적으로 자동실행 레지스트리를 등록하는 등의 행위는 이루어지지 않습니다. 다운받아질 때 유지를 위한 작업이 이루어지고 이러한 프로그램은 단지 광고를 하는 역할만을 충실히 수행합니다.

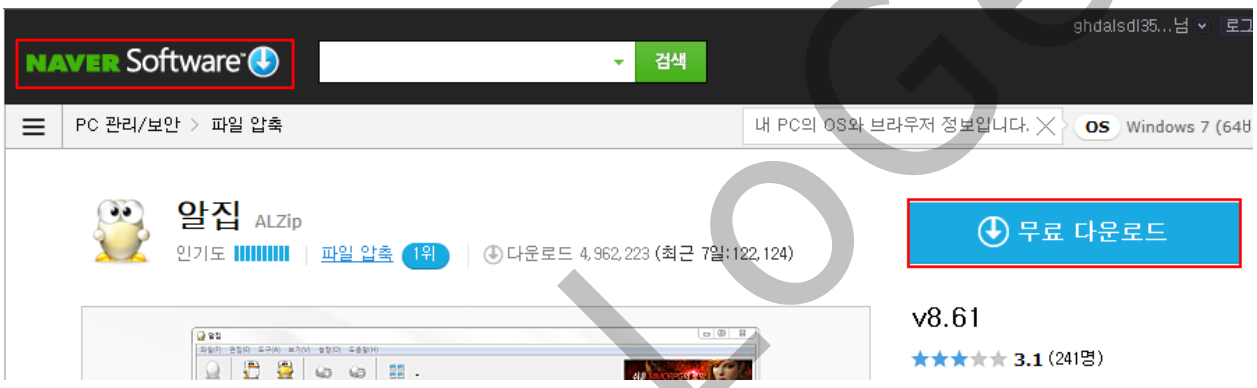
예방법

위에서 말했던 것과 같이 일반 사용자가 흔히 겪게 되는 애드웨어처럼 보이는 형태의 프로그램들은 실제로는 제휴마케팅사이트와 우리가 다운받는 사이트간의 협약에 의해 이루어진 합법적인 프로그램이다.

뭐...자본주의 사회에서 저런 행위를 욕 할 수는 없으니 불편을 겪지 않으려면 다운받을 때 조심하자.

아래에서 하나의 예를 보여준다.

사례: Naver Software 를 이용한 다운로드



우선 시작부터 네이버 툴바 설치에 체크가 돼 있다. 쓸대없이 설치할 필요없다. 체크 해제하자.

아래는 설치할 때 동의사항에 적혀 있는 내용이다.

5. 자동 업데이트

5.1. 본 "제품"에는 업데이트를 위한 정상 작동의 일부로서 인터넷을 통해 통신을 실행 하는 기능이 내장되어 있습니다. 자동 업데이트에서는 필요에 따라 임의의 파일이 "사용자"의 컴퓨터에 설치되며, 이 방식은 임의로 변경 될 수 있습니다. 또한 설치 전 "사용자"의 동의를 별도로 구하지 않으며 이 계약에 동의함으로써 갈음합니다.

5.2. 알약의 경우 위화하 서비스를 외해 다음과 같이 자동 업데이트를 지해

6. 기타 서비스 제공

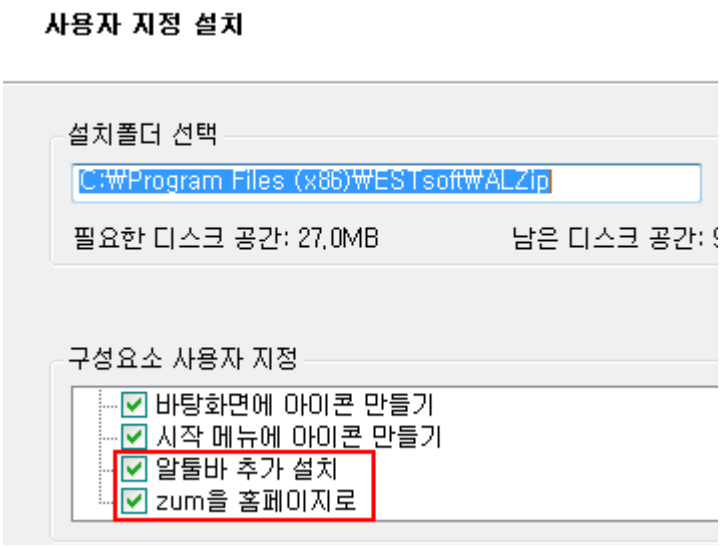
6.1. "회사"는 사용자가 "제품"을 설치 또는 업데이트 시 사용자에게 "제품" 이외의 추가 서비스를 직접 제공할 수 있으며, 사용자는 설치 또는 업데이트를 함으로써 해당 서비스를 제공받는 것에 동의한 것으로 간주됩니다.

6.2. "회사"는 "회사"가 제공하는 서비스나 설정 사항 등을 타사의 제품이나 서비스에서 변경하지 못하도록 차단하거나 방해하는 경우 이를 유하하거나 정

이러한 조항들이 있기 때문에 이런 프로그램에서 설치되는 광고성 추가 프로그램은 불법이아니다..—,—

설치를 한 단계 할 때마다 이런 내용은 포함 돼 있다.

사용할 일 없다면 체크해제하자.(우리가 zum 을 홈페이지로 할 일이 뭐가 있다고...)
그리고 설치 할 때 빠른 설치가 아닌 **사용자 지정**으로 선택하자.



앞에서 사용하기 싫은 내용을 아무리 체크 해제해도 마지막까지 함정이 마련되어있다....
이런 곳에서 제공하는 다운로드를 이용 할 경우 꼭 사용자 정의를 통해 필요 없는 프로그램이 설치되지 않도록 하자. 실제로 지금의 예에서는 툴바나 시작페이지 변경이지만 위에서 봤던 광고성 프로그램도 이런 방식으로 설치가 된다.