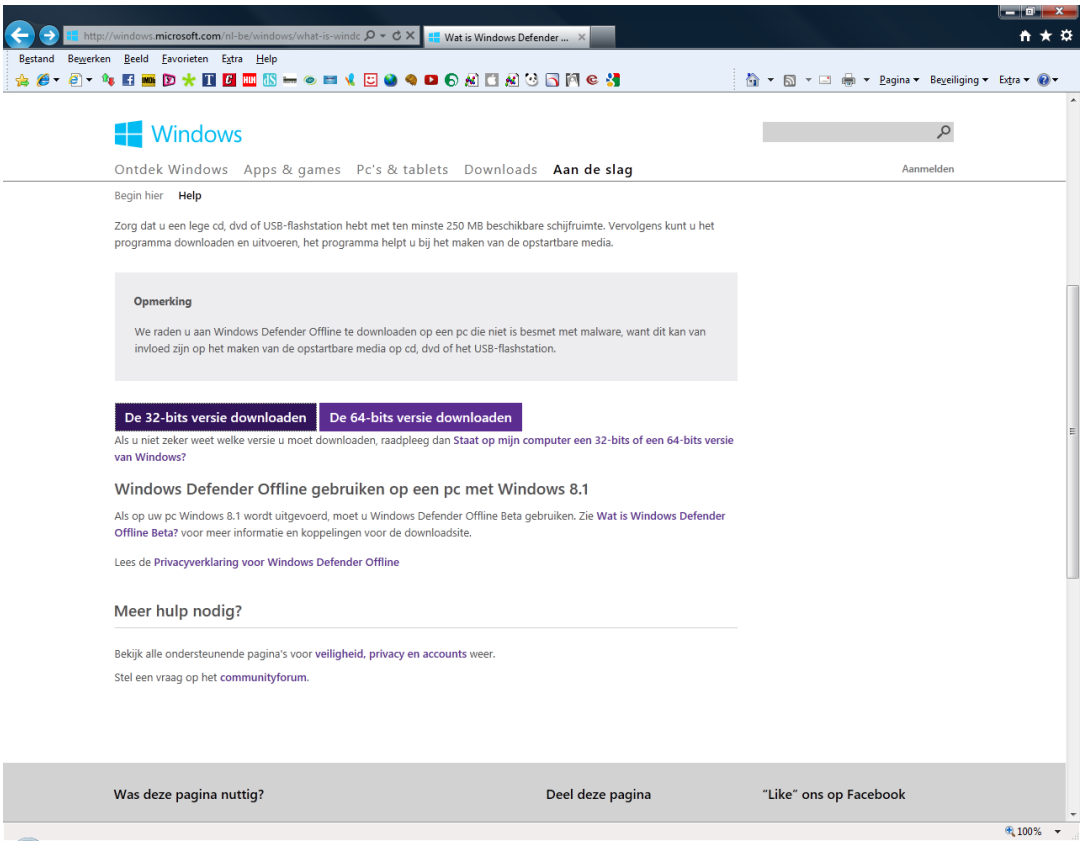
Windows Defender Offline 15/11/2014

Windows Defender Offline is een anti-virus tool van Microsoft waarmee PCs kunnen gescand worden zonder dat Windows opgestart is (het is dus een boot-CD of USB-stick). Virussen of andere malware zitten soms zodanig diep in Windows "verborgen" dat gewone anti-virusscanners die vanuit Windows opgestart worden, ze niet kunnen vinden. Door vanaf een speciale CD of USB-stick op te starten, kan je soms malware vinden die vanuit Windows niet gedetecteerd kon worden.

1. Boot-CD of USB-stick aanmaken

Surf op een niet-besmette PC naar onderstaande website (of zoek in Google naar "Windows Defender Offline") :

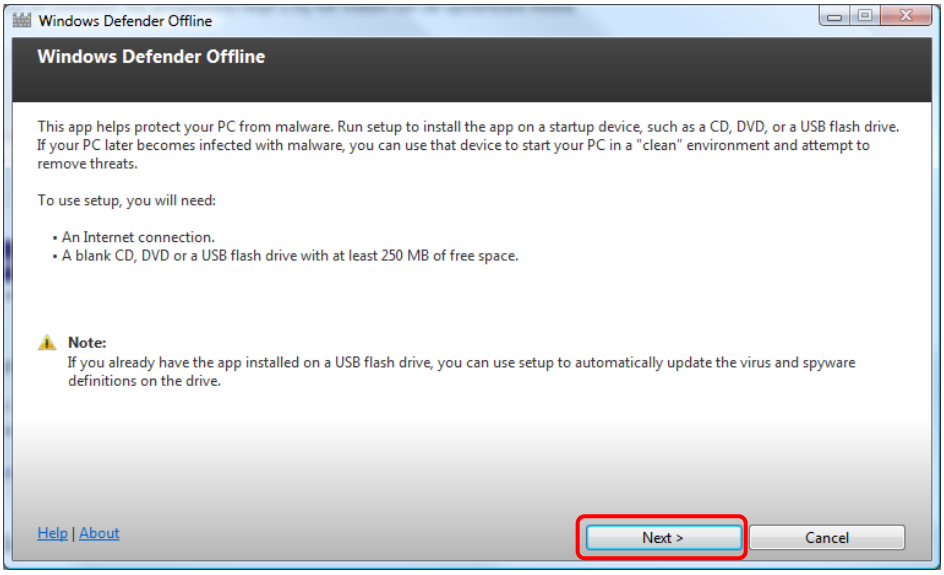
http://windows.microsoft.com/nl-be/windows/what-is-windows-defender-offline

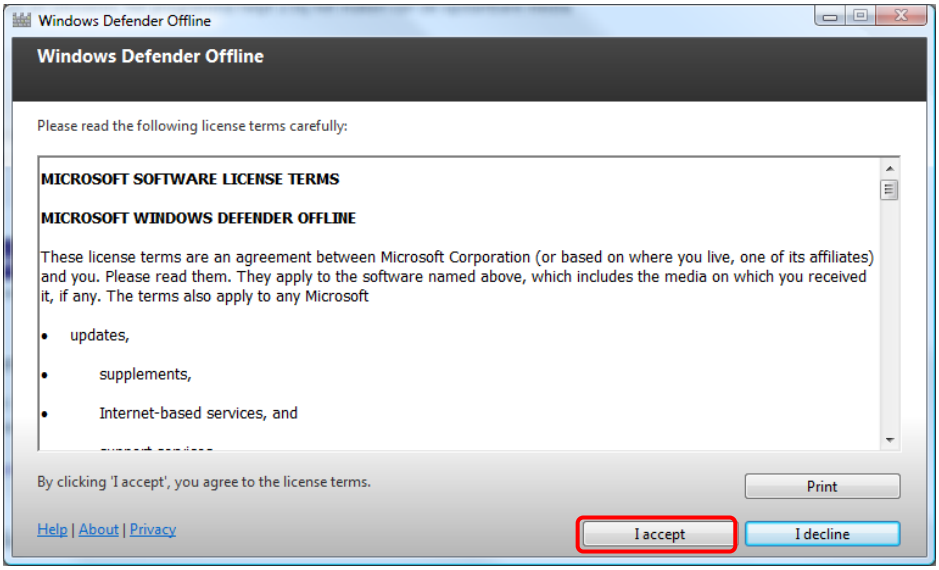


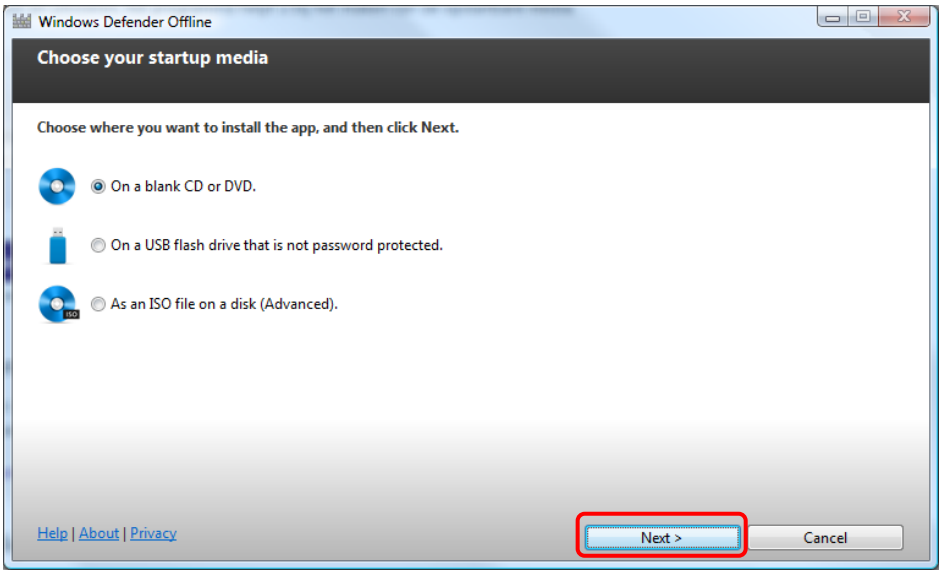
⇨ Kies hier de **32-bit** of **64-bit** versie, naargelang de Windows-versie die er **op de besmette PC** staat (dus niet op de PC waarop u deze boot-CD of USB-stick aanmaakt, maar op de PC die u wilt scannen, dat kan verschillend zijn).

Opm.: mocht u niet weten welke Windows-versie u precies hebt, kijk dan hier eens : http://www.iphelp.be/ftp-labo/procedures/Windows-versie.pdf

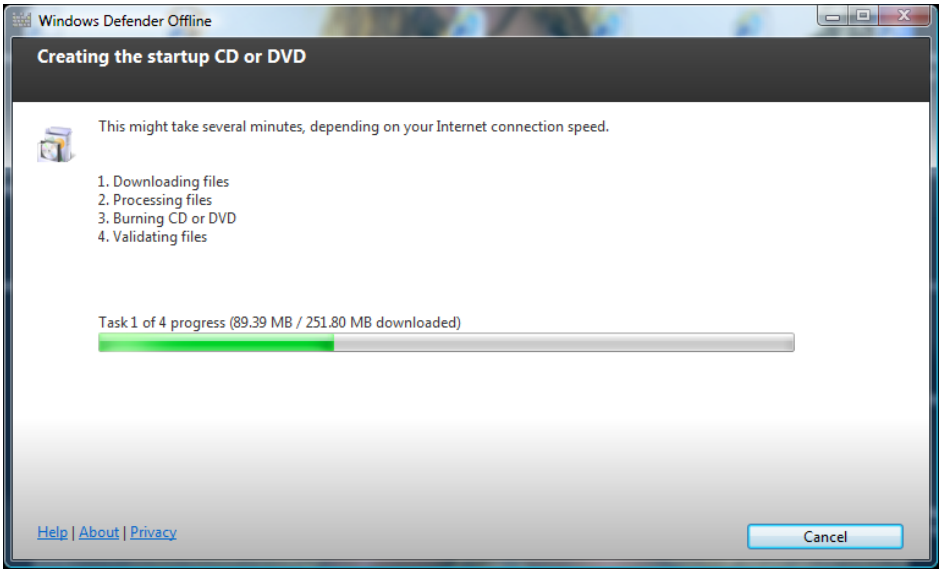
⇨ In dit voorbeeld zal ik een PC scannen waarop 32-bit Windows XP staat en ik zal daarvoor een boot-CD aanmaken : klik daarvoor dus op de 32-bit versie en kies daarna "**Uitvoeren**" :

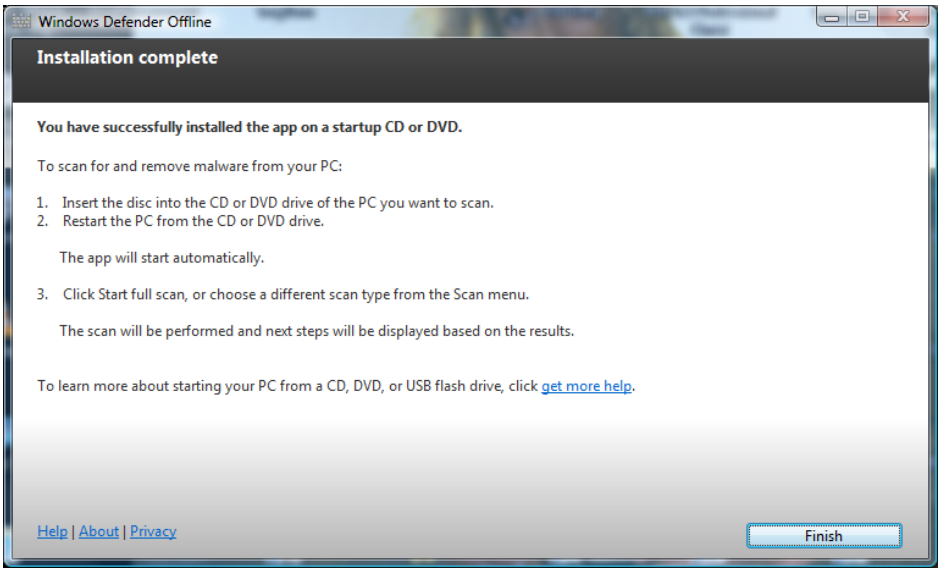






Ik kies dus voor een blanco CD, maar dat mag ook een lege USB-stick zijn.





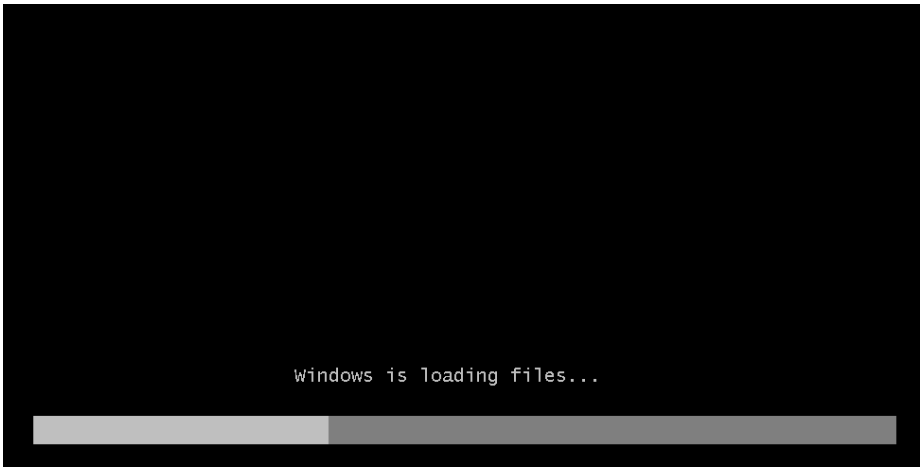
Hiermee is de boot-CD dus klaar.

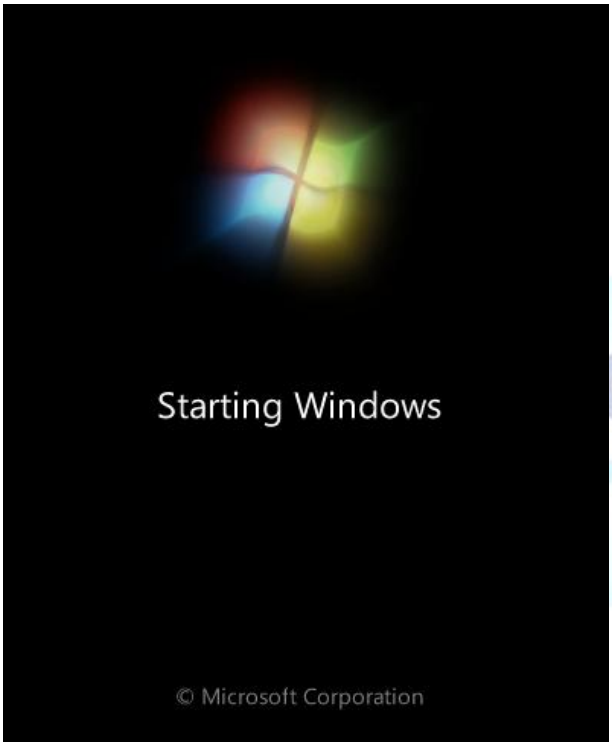
2. Besmette PC scannen

Steek deze CD nu in de (vermoedelijk) besmette PC en start die PC op.
Het is de bedoeling van de PC te laten opstarten vanaf deze boot-CD : bij veel PCs zal hij vanzelf zien dat er een boot-CD in zit en die opstarten, bij sommige PCs moet men specifiek aangeven dat hij vanaf de CD moet opstarten : bij Fujitsu PCs en TOSHIBA portables is dat door meteen na het aanzetten van de PC meerdere keren op de functietoets **F12** te drukken, totdat hij een bootmenusysteem geeft waarin u dan aangeeft dat hij **vanaf CD of DVD moet opstarten**.

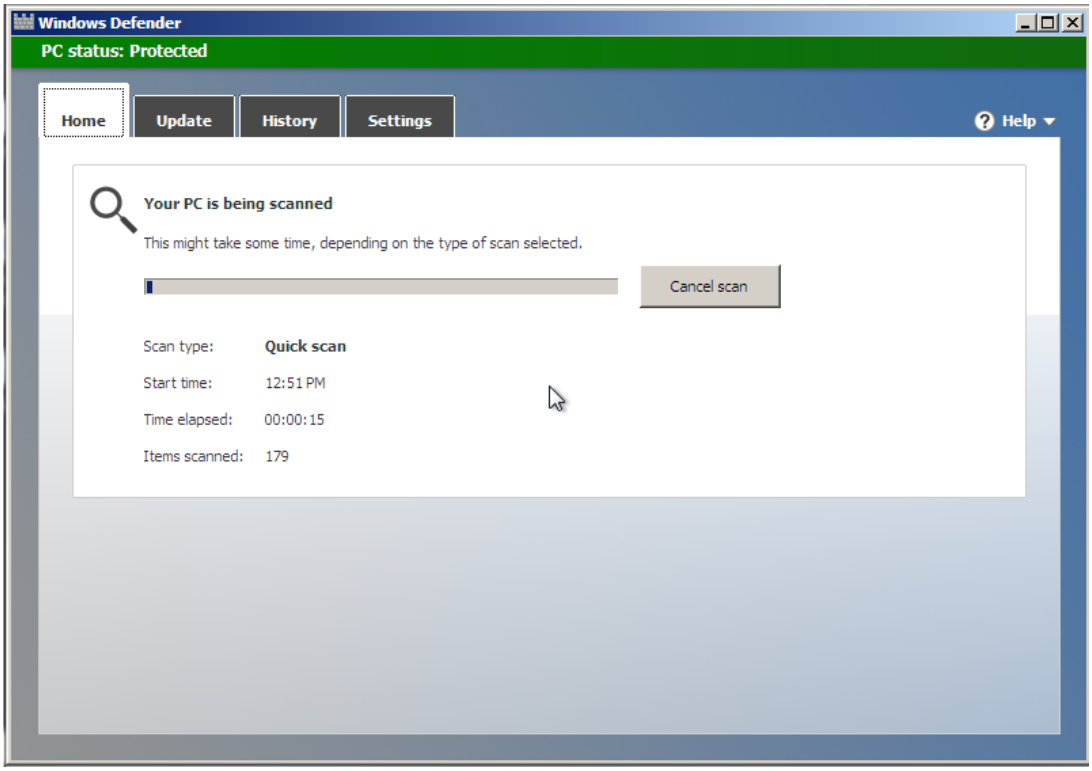
Als hij van CD begint te starten, dan ziet u dit :

Wellicht toont hij nog eerst vrij kort (dus goed opletten !) : “**press any key to boot from CD or DVD**” => druk hier dus op eender welke toets om hem te laten verder gaan.

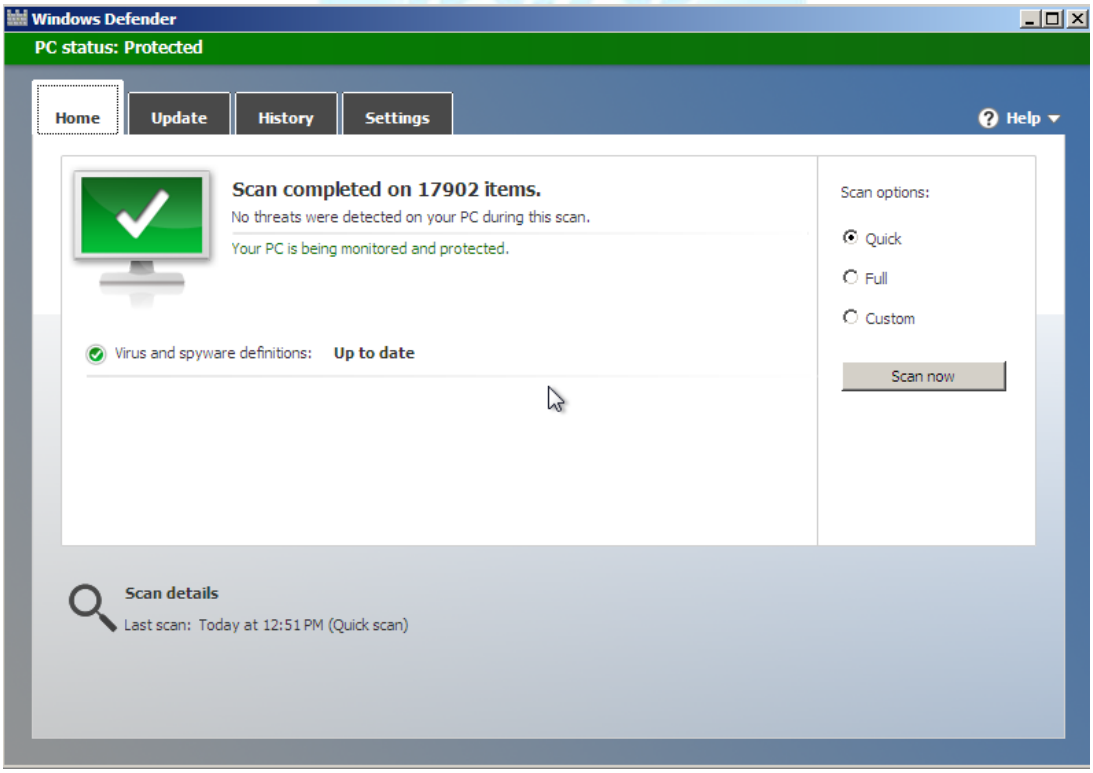




Dit ganse proces duurt een paar minuten. Uiteindelijk geeft hij dit :



Waarschijnlijk begint hij dan meteen te scannen, wat OK is als u deze boot-CD of USB-stick nog maar pas aangemaakt hebt. Mocht u deze boot-CD of USB-stick enige tijd geleden aangemaakt hebben, dan dient u hem eerst nog te updaten, zodat de meest recente malwaresignaturen erop gedownload kunnen worden. Kies daarvoor “Cancel scan” en klik dan op Update en start daarna manueel de scan.



Na het scannen geeft hij aan of hij iets gevonden heeft of niet.

Noteer ev. wat hij gevonden heeft of neem er een foto van voor mochten wij dat later nodig hebben.

Mocht deze scan nog niet volstaan, dan kunt u ev. daarna ook nog eens een **Full scan** doen : die duurt een stuk langer, maar controleert alle bestanden op uw PC.

Deze Microsoft Windows Defender Offline kan niet alle virussen en spyware e.d. detecteren (geen enkel programma kan dat omdat er steeds maar bijkomen), maar omdat hier niet vanuit Windows gescand wordt, is de kans groter dat rootkits e.d. die “onder” Windows kruipen, gevonden en verwijderd kunnen worden.

Als uw PC daarna terug “normaal” opstart, dan doet u voor de zekerheid toch best nog een aantal extra scans vanuit Windows, vb. met Hitman Pro, Bitdefender, MalwareBytes. Zie onze handleidingen daarvoor op http://www.iphelp.be/basiscontrole.html