Federal Computer Crime Unit

Fenomeenfiche

Ransomware

Disclaimer:

De informatie wordt aangeboden als dienstverlening aan slachtoffers van de diverse vormen van infecties met kwaadaardige software die zich voordoet als de politie.
De politie is op geen enkele wijze betrokken bij deze vorm van besmetting en blokkering.
De hierbij gevoegde methodes en oplossingen om geblokkeerde PC's te deblokkeren zijn louter informatief.
Hoewel de vermelde methodes door de politie werden uitgetest en geschikt werden gevonden in een beperkt aantal testopstellingen, kan de politie op geen enkele wijze de effectieve oplossing garanderen voor alle mogelijke situaties.
Het toepassen van de voorgestelde methodes door slachtoffers gebeurt op hun eigen verantwoordelijkheid.
De politie kan onder geen enkele voorwaarde aansprakelijk worden gesteld voor enige schade die aan een PC zou kunnen ontstaan ten gevolge van het toepassen van de voorgestelde technieken.

Verantwoordelijke uitgever

Federal Computer Crime Unit - FCCU
Directie economische
en financiële criminaliteit
Federale gerechtelijke politie

Klik hier als u slachtoffer bent?

NL Versie : 11/09/2012 9:14:20

1 Fenomeenomschrijving

Ransomware betreft een kwaadaardige software (malware) die de computer van het slachtoffer blokkeert. Meestal wordt er een betaling gevraagd om de machine te deblokkeren wat echter in de meeste gevallen niet helpt.

(Voorbeeld van een recente ransomware)

2 Wijze van verspreiding – schadelijke effecten

Het malware-bestand kan zich bevinden in een ontvangen e-mail (als bijlage) maar kan evengoed ingewerkt zijn in een webpagina. Tegenwoordig worden deze bestanden ook verspreid via linken en filmpjes op sociale netwerksites zoals Facebook, Netlog, Google+, enz…

De e-mailvariant bevat meestal een .pdf, .zip of .exe bijlage waarbij uiteraard gevraagd wordt deze open te klikken.
Nadat men hierop heeft geklikt zal zich een document openen met voor de ontvanger weinig relevante informatie.
Op dat ogenblik wordt er een virus of Trojaans paard geïnstalleerd op uw computer.
Vanaf dan kan alle gevoelige informatie (wachtwoorden, kredietkaartgegevens, ...) zonder dat u het beseft, worden doorgestuurd naar de cybercriminelen.

3 Wat te doen om te voorkomen dat u slachtoffer wordt?

Voorzie uw computer van een antivirusprogramma dat regelmatig wordt geüpdatet. Op internet zijn verschillende gratis antivirusprogramma's te vinden. Zorg ook dat er een firewall geactiveerd is. Er zit al standaard een firewall in Windows maar het kan geen kwaad daarnaast een alternatieve firewall te installeren. Ook hiervan vind je er gratis op internet.

Zorg er ook voor dat de geïnstalleerde software op uw computer is geüpdatet. Makers van software brengen regelmatig updates uit om beveiligingslekken te dichten (bvb. Microsoft Windows, Acrobat Reader, Flashplayer, enz.).

Tenslotte geldt ook hier: "Gebruik je gezond verstand". Zit er een bijlage in een e-mailbericht waarvan u de afzender niet kent? Verwijder dan die e-mail zonder de bijlage te openen.

4 Wat te doen als u slachtoffer bent?

4.1 Klacht

BETAAL NIET!
Indien u toch betaald zou hebben of u hebt enige vorm van schade opgelopen, wordt u ten zeerste aangeraden om een klacht in te dienen bij de lokale politie wegens verspreiding van malware met het oog op hacking, computersabotage en afpersing.

Als u betaald heeft, neem dan zo snel mogelijk contact op met:

Ukash	**PaysafeCard**
Blokkeren van de PIN via het telefoonnummer :	Blokkeren van de PIN via het telefoonnummer :
- 00 800 000 85274 of	- 078/ 158 157 (hotline op het ticket) of
- 00 800 247 85274	- 00 800 0729 7233
Met de PIN nummer en het bedrag van het ticket	Met de PIN nummer en het bedrag van het ticket.

Neem een foto van alle schermen die u te zien krijgt op uw computer en bewaar deze om bij uw dossier te voegen. Noteer welke acties u laatst op uw computer hebt uitgevoerd en het tijdstip ervan.

4.2 Mogelijke oplossingen (*)

* De hierbij gevoegde methodes en oplossingen om geblokkeerde PC's te deblokkeren zijn louter informatief. Hoewel de vermelde methodes door de politie werden uitgetest en geschikt werden bevonden in een beperkt aantal testopstellingen, kan de politie op geen enkele wijze de effectieve oplossing garanderen voor alle mogelijke situaties.
Het toepassen van de voorgestelde methodes door slachtoffers gebeurt op hun eigen verantwoordelijkheid. De politie kan onder geen enkele voorwaarde aansprakelijk worden gesteld voor enige schade die aan een PC zou kunnen ontstaan ten gevolge van het toepassen van de voorgestelde technieken.

Naargelang uw kennis van computersystemen kunt u de volgende mogelijkheden uitproberen:

1. Mogelijkheid 1: contact opnemen met een computertechnicus (computerwinkel)
2. Mogelijkheid 2: proberen deblokkeren via de Veilige Modus
3. Mogelijkheid 3: proberen deblokkeren via een opstart-CD of -USB
    - Benodigdheden voor de 3de optie
        - Niet geïnfecteerde computer verbonden met het internet
        - USB of CD-drive

4.2.1 Mogelijkheid 2: Veilige Modus

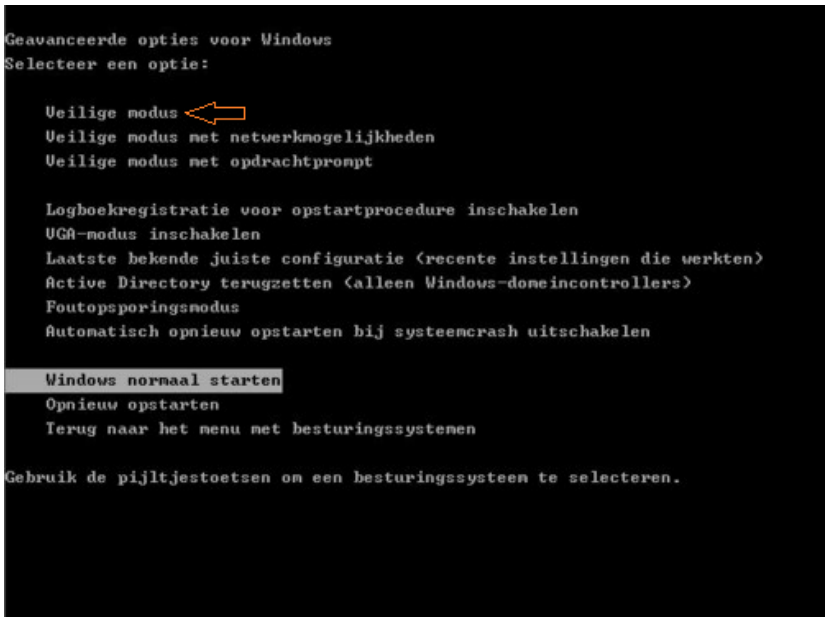
Naast een bezoek aan de plaatselijke computerwinkel, kunt u uw computer opnieuw opstarten in Veilige Modus. Uw Windowsprogramma zal dan worden gestart met een beperkte set bestanden en stuurprogramma's.
Hoe gaat u te werk?

A. Veilige Modus

1. Verwijder alle diskettes, cd's en dvd's uit uw computer en start uw computer vervolgens opnieuw op.
2. Houd de toets F8 

ingedrukt terwijl de computer opnieuw wordt gestart. U moet op de toets F8 drukken voordat het Windows logo wordt weergegeven. Als het Windows logo toch verschijnt, moet u wachten totdat de aanmeldingsprompt van Windows wordt weergegeven, de computer uitschakelen, opnieuw starten en het vervolgens opnieuw proberen.

3. U bent nu in het scherm "Geavanceerde opstartopties". U kunt nu met de pijltjestoets scrollen naar 'Veilige Modus" of "Safe Mode". Vervolgens drukt u op ENTER.

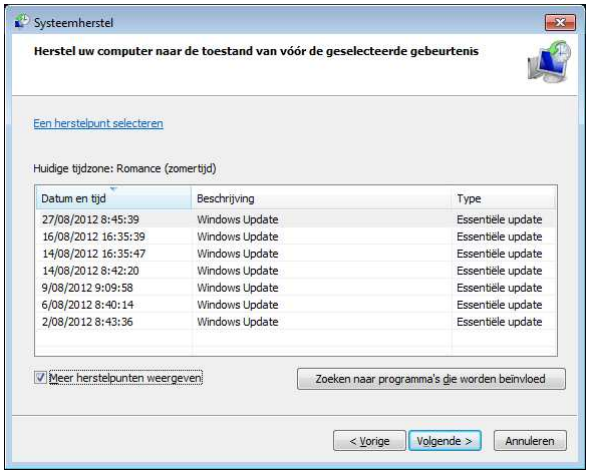


Als alles goed verloopt zal Windows nu in "Veilige Modus" opstarten zonder dat het scherm van de ransomware zal laden.

B. Herstelpunt terugzetten

a) **Indien Windows 7 of Windows Vista**
Klik op de startknop en typ "herstel" in het zoekvakje. In de lijst met zoekresultaten klikt u vervolgens op "Deze computer naar een eerdere toestand herstellen" en vervolgens op "Systeemherstel starten". Deze methode zal uw persoonlijke bestanden (bijvoorbeeld foto's of documenten opgemaakt in MS Office) ongemoeid laten, hoewel het maken van een externe back-up altijd aan te raden is. Het is mogelijk dat Windows vraagt naar uw beheerderspaswoord of gewoon vraagt op de bevestigingsknop te klikken.

1. Met behulp van de Wizard kunt u nu een herstelpunt kiezen. Eventueel kunt u het vakje aanvinken waar "Meer herstelpunten weergeven" staat.



2. Klik dan op volgende en na uw bevestiging zal de computer de vorige configuratie herstellen en opnieuw opstarten.

b) Indien Windows XP

1. Klik op de Start knop.
2. Vervolgens ga je naar Accessoires > Systeem Werkset > Systeemherstel.
3. Kies dan de optie "Een eerdere status van deze computer herstellen" en klik op "Volgende".
4. Selecteer een recent herstelpunt in de lijst of klik op een in het vet staande datum in het kalendertje. Klik dan op "Volgende".
5. Bevestig en klik op "Volgende", de computer zal de gekozen configuratie herstellen en zal nadien herstarten.
6. Nadat de computer is opgestart en u bent ingelogd zal u opnieuw een venster krijgen met de melding dat het systeemherstel uitgevoerd werd. U dient dan op "OK" te klikken.

Voor Windows XP zie ook: http://files.computertotaal.nl/2008/workshops/XP-Een-herstelpunt-terugzetten.htm

C. Scannen met antivirus/antimalware programma

Nadat uw computer opnieuw is opgestart zal u in de normale Windows omgeving terecht komen.

Dit betekent niet dat het virus of andere kwaadaardige bestanden volledig verwijderd werden.

Het is dan ook ten zeerste aan te raden uw computer nu te scannen met een up to date antivirusprogramma.
Gebruik de optie "Volledige scan". Let op, deze scan kan enkele uren duren.

4.2.2 Mogelijkheid 3: Windows Defender Offline

Een derde mogelijke oplossing om uw computer te deblokkeren, is gebruik maken van de gratis software "Windows Defender Offline" (uitgegeven door Microsoft).

Benodigdheden:
- Een niet-geïnfecteerde computer verbonden met het internet
- Een USB-stick

Systeemvereisten:
Zowel de pc die is besmet met een virus of malware als de pc die wordt gebruikt voor het maken van opstartbare media, dienen te voldoen aan de volgende systeemvereisten.

Besturingssysteem:

- Windows XP Service Pack 3
- Windows Vista, Windows Vista met SP1, Windows Vista met SP2 of hoger
- Windows 7, Windows 7 met SP1 of hoger
- Windows Developer Preview, Windows 8 Consumer Preview

Geheugen:

- Windows XP: 512 MB RAM of meer
- Windows Vista, Windows 7, Windows Developer Preview: 1 GB RAM of meer

Videoresolutie: 800 X 600 of hoger

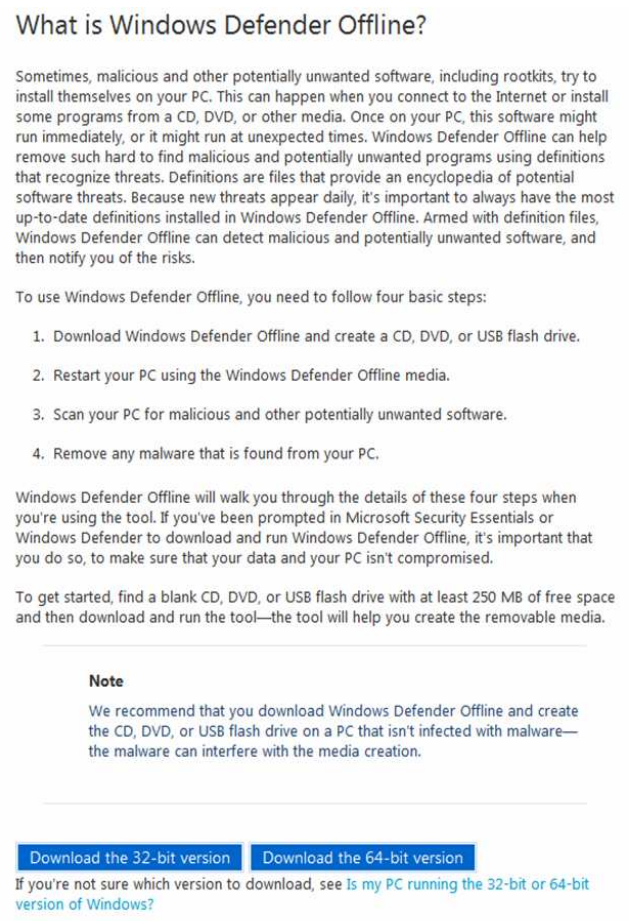
Beschikbare schijfruimte: 500 MB

Op de volgende website kan u de gratis software "Windows Defender Offline" downloaden:
http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1

Deze software downloadt u vanop de niet-geïnfecteerde computer. De software is bedoeld om een USB-stick aan te maken waarmee u de besmette computer kan opstarten. De software zal dan de computer scannen op virussen en malware.

Verdere stappen:

Stap 1. Download de juiste versie van de software in functie van het besturingssysteem van de geïnfecteerde computer (32 bit of 64 bit):
http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1



What is Windows Defender Offline?

Sometimes, malicious and other potentially unwanted software, including rootkits, try to install themselves on your PC. This can happen when you connect to the Internet or install some programs from a CD, DVD, or other media. Once on your PC, this software might run immediately, or it might run at unexpected times. Windows Defender Offline can help remove such hard to find malicious and potentially unwanted programs using definitions that recognize threats. Definitions are files that provide an encyclopedia of potential software threats. Because new threats appear daily, it's important to always have the most up-to-date definitions installed in Windows Defender Offline. Armed with definition files, Windows Defender Offline can detect malicious and potentially unwanted software, and then notify you of the risks.

To use Windows Defender Offline, you need to follow four basic steps:

1. Download Windows Defender Offline and create a CD, DVD, or USB flash drive.
2. Restart your PC using the Windows Defender Offline media.
3. Scan your PC for malicious and other potentially unwanted software.
4. Remove any malware that is found from your PC.

Windows Defender Offline will walk you through the details of these four steps when you're using the tool. If you've been prompted in Microsoft Security Essentials or Windows Defender to download and run Windows Defender Offline, it's important that you do so, to make sure that your data and your PC isn't compromised.

To get started, find a blank CD, DVD, or USB flash drive with at least 250 MB of free space and then download and run the tool—the tool will help you create the removable media.

Note

We recommend that you download Windows Defender Offline and create the CD, DVD, or USB flash drive on a PC that isn't infected with malware—the malware can interfere with the media creation.

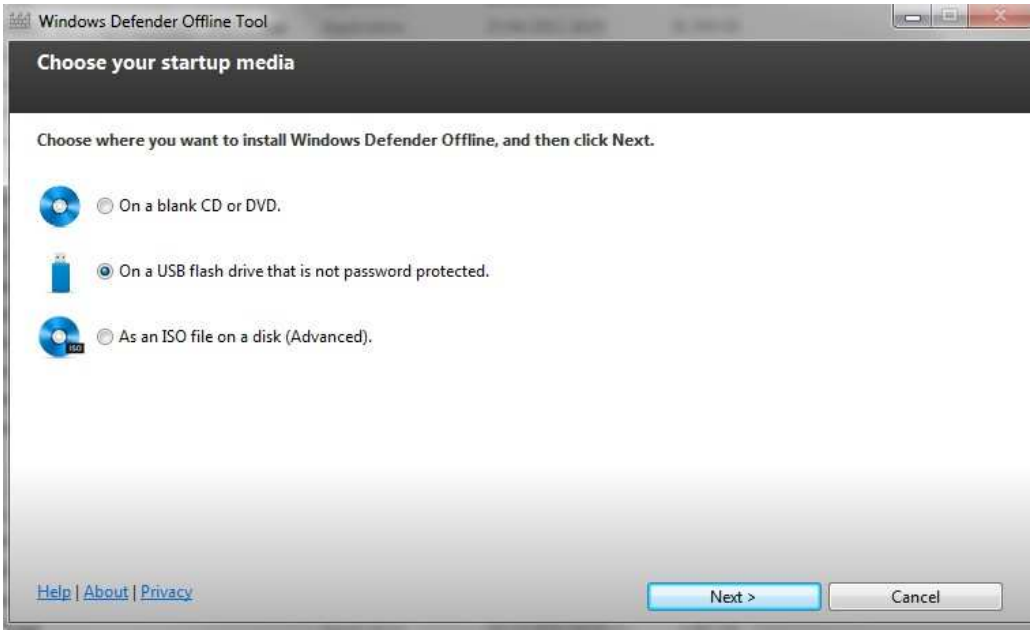
Download the 32-bit version | Download the 64-bit version

If you're not sure which version to download, see Is my PC running the 32-bit or 64-bit version of Windows?

Stap 2. Voer vervolgens de software uit. U krijgt dan volgend scherm:

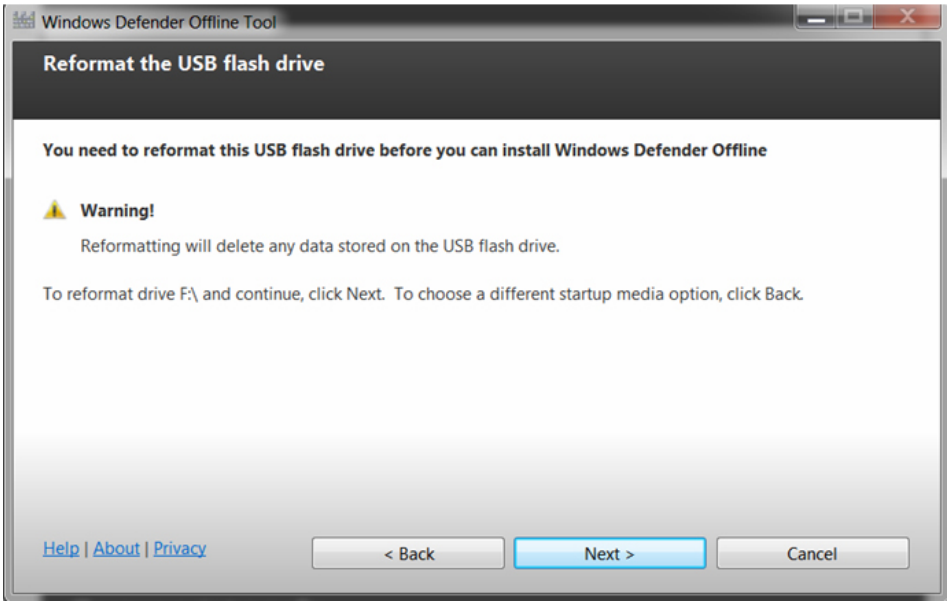
Klik op Next.

Stap 3. Steek vervolgens de USB-stick in de computer. Let op dat er geen gegevens op deze USB-stick staan want deze wordt geformatteerd.



U hebt de keuze om verschillende media te beschrijven. Wij opteren hier voor een USB-stick, de 2de keuze in het scherm.

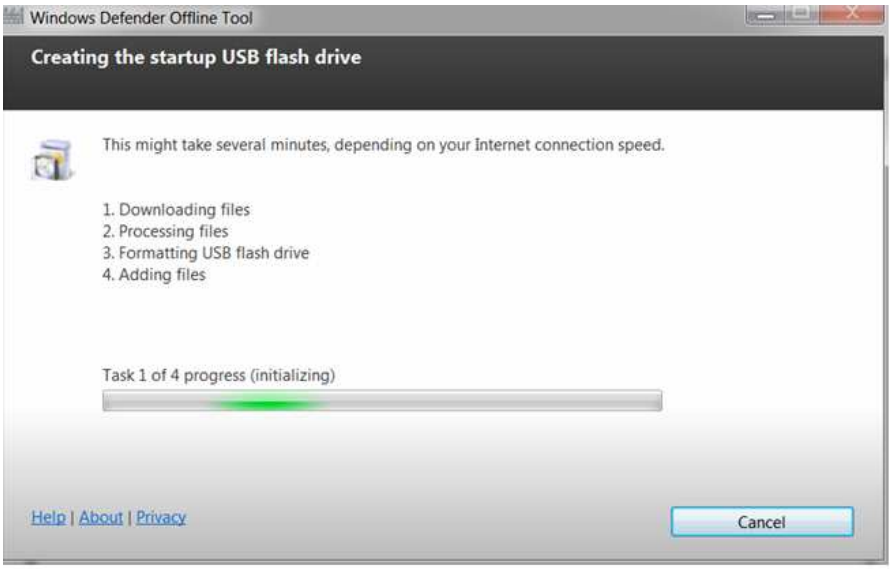
Klik op Next.



U wordt gewaarschuwd dat de USB-stick zal worden geformatteerd.

Klik op Next.

Stap 4. De opstart-USB-stick wordt nu aangemaakt.



Wanneer stap 4 is bereikt, hebt u een opstart-USB-stick aangemaakt. D.w.z. dat u hiermee uw geblokkeerde computer kunt opstarten.

Stap 5. De geïnfecteerde computer virus- of malwarevrij maken

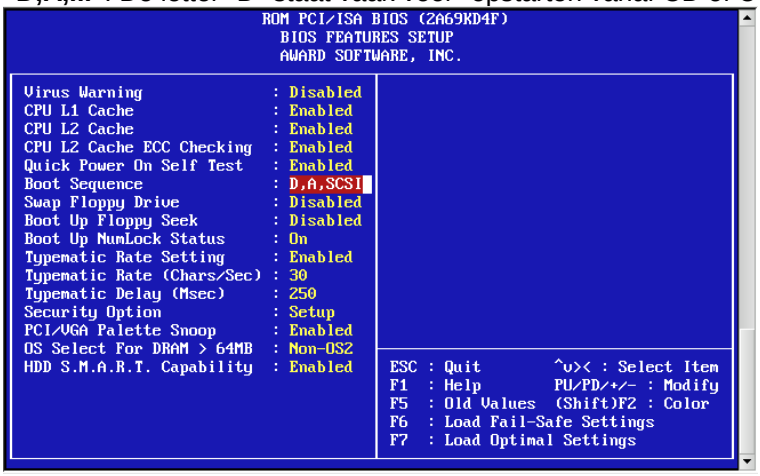
Wanneer u een opstart-USB wilt gebruiken, dient u eerst in het BIOS er voor te zorgen dat de computer kan opstarten vanop een USB-stick.

Het BIOS (Basic Input/Output System) is een programma dat in pc's is ingebouwd en waarmee het besturingssysteem wordt gestart wanneer u de computer inschakelt.
Wees voorzichtig wanneer u de BIOS-instellingen wijzigt. De BIOS-interface is ontworpen voor ervaren gebruikers en als u een instelling wijzigt, bestaat de kans dat de computer niet meer juist kan

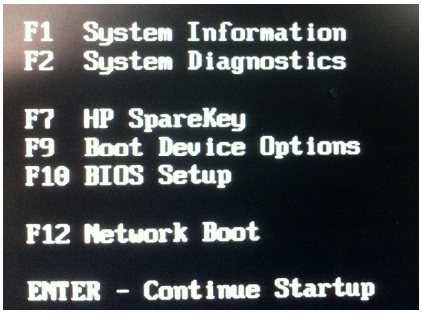
worden opgestart. Indien u niet zeker bent, kunt u beter beroep doen op iemand met kennis van zaken.

Hoe kom ik in het BIOS terecht?
De procedure verschilt per BIOS-fabrikant. Meestal moet u op een toets (zoals F2, F12, DEL, ESC) of toetsencombinatie drukken nadat u de computer hebt ingeschakeld, maar voordat Windows wordt gestart. Vervolgens gebruikt u de pijltjestoetsen om naar "Boot Sequence" of naar de tab "Boot" te gaan.

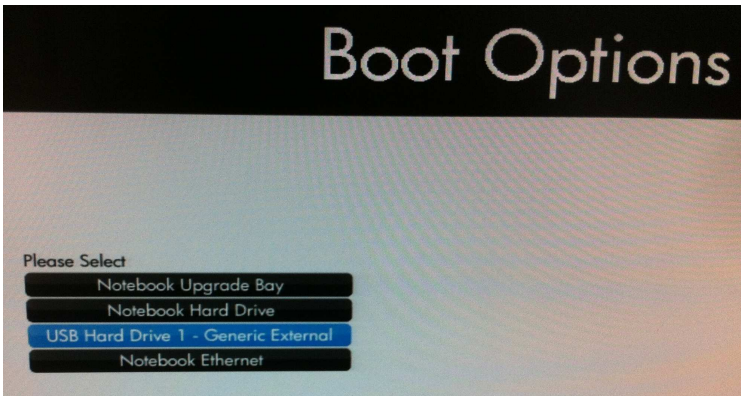
We geven hier 2 voorbeelden :
Bij iets oudere computers dient de opstartvolgorde (boot sequence) veranderd te worden naar **"D,A,..."**. De letter "D" staat vaak voor "opstarten vanaf CD of USB".



Bij recentere computers kan u het volgende tegenkomen:
Nadat u op de toets gedrukt hebt om toegang te krijgen tot het BIOS (F2, F12, DEL, ESC), krijgt u een menu:



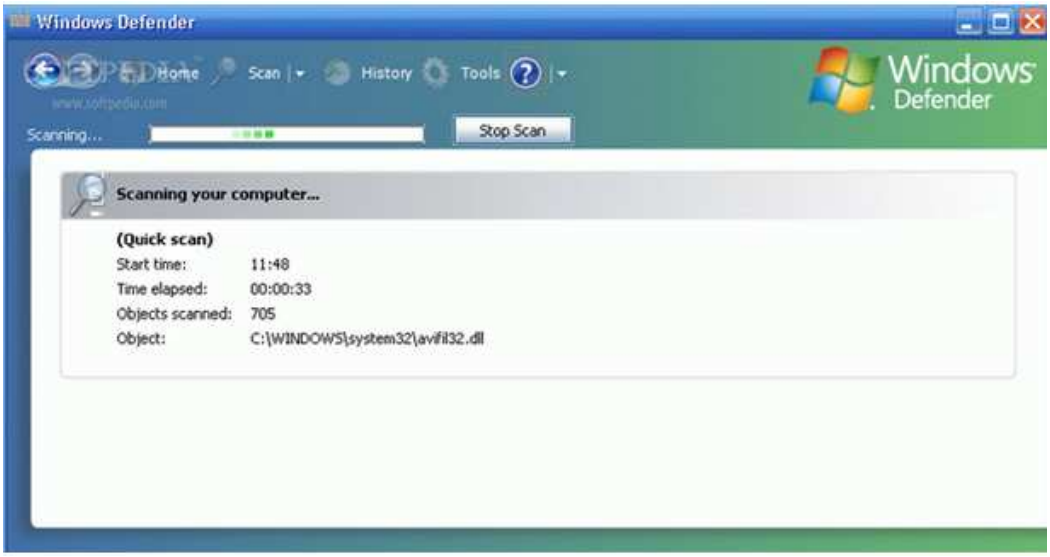
Na op de functietoets F9 gedrukt te hebben worden de Boot Device Options getoond:



U plaatst dan de door Windows Defender Offline gemaakte opstart-USB-stick in een USB-poort en selecteert USB hard Drive 1 (of een gelijkaardige aanduiding met USB) uit het opstartmenu.

Als de BIOS juist is ingesteld, en de USB-stick steekt in, zal de computer opstarten vanaf de USB-stick en wordt het scannen naar malware gestart.

Indien alles correct is ingesteld en de computer start niet op vanop de USB-stick, probeer dan nogmaals nadat u de stick in een andere USB-poort gestoken hebt.



Wanneer de scan is voltooid, start uw computer opnieuw normaal op.

4.3 Maatregelen

Wanneer uw computer opnieuw normaal is opgestart dient u wel nog een volledige scan uit te voeren met een up-to-date antivirusprogramma.
Als u 100% gerust wil zijn kunt, u best het Windows besturingssysteem herinstalleren.