

Het DNSChanger virus

Over wat gaat het ?

Het Belgische computernetwerk wordt bedreigd door een virus dat op 7 maart tal van computers in ons land kan afsluiten van het internet. Dat meldt de federale overheidsdienst CERT.

Het Computer Emergency Response Team is een team van ICT'ers dat in staat is snel te handelen als zich een beveiligingsincident voordoet met computers of computernetwerken. Het virus waarvoor de dienst waarschuwt heeft intussen al 4 miljoen computers aangetast in meer dan honderd landen, en volgens het CERT is het waarschijnlijk dat het ook België in zijn greep heeft. Het Cert kan evenwel de impact van het virus, DNSChanger genaamd, nog niet inschatten.

De dienst vraagt daarom elke computergebruiker in ons land om vóór 7 maart even naar de website www.dns-ok.be te surfen om te zien of het virus de computer heeft aangetast en, als dat het geval is, het te verwijderen.

Dat virus komt voort uit de online-fraude van zes Estse hackers die erin slaagden om miljoenen computers te kraken en de internetverbinding meteen om te buigen naar gerichte advertentiewebsites. Na twee jaar onderzoek door de FBI kon de bende worden opgepakt.

'Momenteel is het gevaar geweken, omdat de FBI een voorlopige server heeft geïnstalleerd die de impact van het virus ondermijnt'. 'Maar die server verdwijnt op 7 maart. Geïnfekteerde computers zullen op dat moment geen toegang meer hebben tot het internet

Uitleg over het virus DNSChanger

1. Wat doet dit virus?
2. Waarom kan ik bij besmetting door het virus "DNSChanger" mogelijk vanaf 7 maart 2012 niet meer op het internet surfen?
3. Wijzigt CERT.be iets aan mijn computer als ik de test doe op www.dns-ok.be?

1. Wat doet dit virus?

In het kort:

Het virus "DNSChanger" past op uw computer uw internetinstellingen aan.

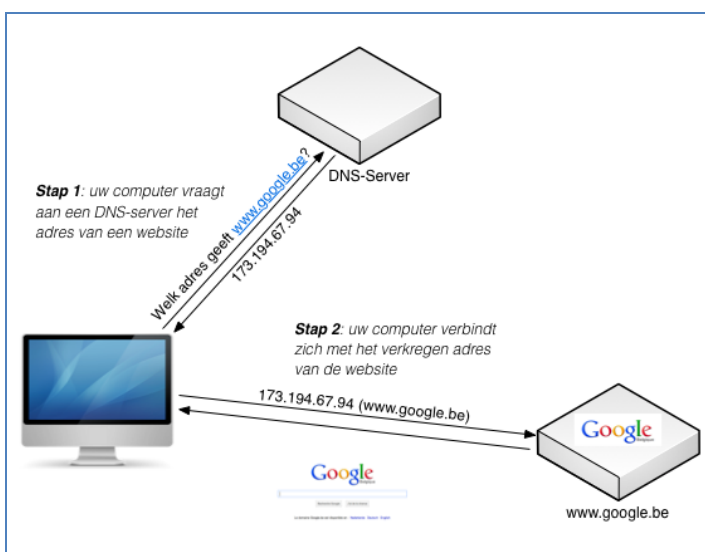
Zo belandde u op vervalste websites met als doel gegevens te stelen of op websites met advertenties waarmee de internetcriminelen geld verdienen. U dient enkel uw computer(s) te checken. Het virus "DNSChanger" was immers enkel gericht op computers (dus niet op smartphones, tablet-computers en dergelijke).

In detail:

Op het internet heeft elke computer en elke website een adresnummer ("IP-adres") dat kan vergeleken worden met een adres of een telefoonnummer. Als u wil surfen naar bijvoorbeeld *www.google.be* dan gaat uw computer op zoek naar het adres van deze website.

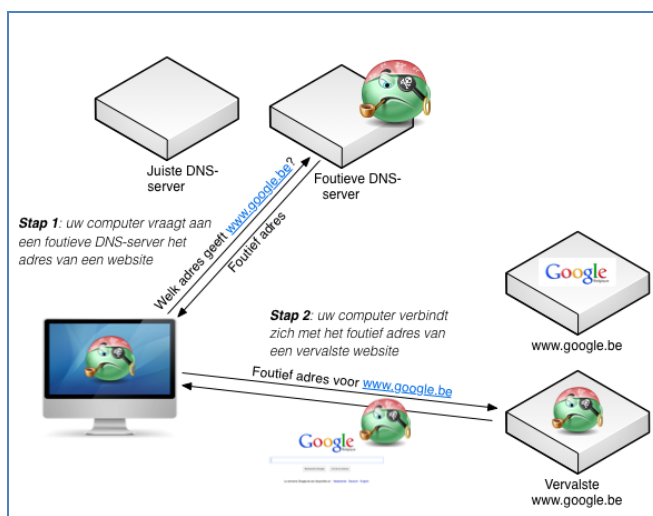
Uw computer zoekt de website via een zogenaamde "DNS-server". De DNS-server zal uw computer doorgeven dat *www.google.be* overeenkomt met een bepaald IP-adres (zoals bijvoorbeeld in het schema hieronder *173.194.67.94*).

U kunt dit dus vergelijken met het zoeken naar een persoon in de telefoongids: u zoekt de naam en u krijgt het telefoonnummer dat u vervolgens kan bellen.



Uw internetleverancier geeft uw computer automatisch aan welke DNS-server hij moet gebruiken om een website op te roepen.

Het virus “DNSChanger” probeert echter de instellingen over de DNS-server op uw computer te wijzigen. Hierdoor maakt uw computer gebruik van een foutieve DNS-server. Zo kwamen besmette computers terecht op vervalste websites met als doel gegevens te stelen of op websites met advertenties waarmee de internetcriminelen geld verdienen.



2. Waarom kan ik bij besmetting door het virus “DNSChanger” mogelijk vanaf 7 maart 2012 niet meer op internet surfen?

In november 2011 pakte de Amerikaanse FBI de internetcriminelen op die het virus “DNSChanger” hadden ontwikkeld. De FBI nam toen de foutieve DNS-servers van de internetcriminelen over. Deze DNS-servers leidden computergebruikers immers naar vervalste websites of advertenties waarmee de internetcriminelen geld verdienen. De Amerikaanse FBI heeft de foutieve DNS-servers vervangen door tijdelijke DNS-servers waardoor besmette computers niet meer naar vervalste websites worden doorgestuurd.

Op 7 maart 2012 zal de FBI deze tijdelijke DNS-servers definitief afzetten.

Besmette computers zullen dan niet langer op internet geraken.

3. Wijzigt Cert.be iets aan mijn computer als ik de test doe op www.dns-ok.be?

Absoluut niet.

Als uw computer niet besmet lijkt, dan heeft u via de juiste DNS-server op het internet kunnen surfen (zoals in schema A hieronder).

Besmette computers zullen verbinding maken met de tijdelijke DNS-server van de Amerikaanse FBI. Hierdoor weet www.dns-ok.be dat uw computer door het virus "DNSChanger" besmet is (zoals in schema B hieronder). Opgeliet, de test op www.dns-ok.be zegt enkel of uw computer besmet lijkt of niet. Deze test verwijdert het virus "DNSChanger" dus niet. Daarvoor adviseren we u enkele programma's om het virus "DNSChanger" te verwijderen.

Onze adviezen krijgt u te lezen op www.dns-ok.be als uw computer besmet is.

