Google blijft cooler dan Coolwebsearch

Maart 2004

Henk Jongedijk, maandag 23 oktober 2006 - 00:00:00

Uit mijn vorige columns heeft u vast al begrepen dat ik een echte Google fan ben! U mag mij gerust als een Googlist of een Googlomaan betitelen. Ook op virusgebied ben ik reuze nieuwsgierig maar bovenal ook voorzichtig. Dat beide onderwerpen mijn pad zouden kruisen had ik niet verwacht. Op deze gebieden durf ik mezelf bekwaam te noemen, dus ik vermoed dat meerdere mensen wel eens getroffen zouden kunnen worden door dit fenomeen. Hoe kon een voorzichtig persoon nu getroffen worden door een virus? En hoe kon ik het oplossen? Een relaas van een fanatieke Googlaar.

Als een echte op koopjes beluste Nederlander was ik op zoek via naar coupons voor Amazon.com. Ik had namelijk bij het betalen gezien dat je een code kon invoeren om extra korting te krijgen. Die hebberigheid deed me de das om.

Uiteraard zocht ik via Google, en wel naar "amazon promotional claim code".

Op nummer Ã © Ã ©n stond: clackamasliteraryreview.com (Klik hier niet op! Of toets de volgende link niet in uw adresregel van uw webbrowser in!) Ze verwezen door naar pagina: http://clackamasliteraryreview.com/amazon-promotional-claim-code.html

Deze promotie-pagina sluiste mij meteen door naar http://64.237.57.166/

Ik kwam op een pagina terecht met allemaal foto\'tjes van vrouwen waarmee ik live zou kunnen chatten. Dat wilde ik helemaal niet, want dat zocht ik immers niet. Ik ging terug naar Google, maar elke keer als ik zocht kwam ik op een pagina van CoolWebSearch uit... Ook kreeg ik opeens allerlei rare opspringende reclameschermen (de zogenaamde popups). Bij mijn favorieten stonden opeens spontaan links ertussen die ik er nooit aan had toegevoegd... Kortom, mijn alarmbellen waren aan het rinkelen want mij bekroop het gevoel besmet te zijn met een virus.

Het was even zoeken, maar ik ontdekte dat ik werd besmet met het de CoolWebSearch (CWS) hijacker:

Op de site van spywareinfo staat goed uitgelegd wat CoolWebSearch precies is. Ook vond ik op de generation.net website een lange lijst (echt een heleboel!) waar je deze besmetting allemaal op kan lopen (kijk onder het kopje CoolWebSearch - CWS).

Alle belangrijkste kenmerken van de CoolWebSearch (CWS) hijacker:

- CoolWebSearch pagina\'s of aanverwante pagina\'s worden automatisch doorgestart/doorgelinkt
- Doorverlinken eh.. doorlinken naar CoolWebSearch na bezoek aan Google
- Internet Explorer (IE) wordt enorm traag bij typen
- IE heeft als startpagina CoolWebSearch gekregen na een herstart (reboot)
- Ongevraagde links in de favorieten
- Popups in Google en Yahoo tijdens het zoeken
- Fouten over de WIN.INI of EIDLL.EXE bij het opstarten

» Onmogelijk om de startpagina te veranderen of te wijzigen

» De IE opties (options) zijn niet meer te wijzigen

Het was overigens niet te achterhalen wie achter de doorverwezen website zit.... mijn pogingen om informatie hierover op te halen liepen op niets uit.
De CW Shredder hielp me van de pop-ups, de startpagina en de zoekacties tijdens bezoek aan Google af.

Samenvatting

» *probleem*: Google verwijst telkens naar andere zoekmachine CoolWebSearch

» *oplossing*: CW Shredder 1.51 (download van majorgeeks)

» *oorzaak*: mijn Windows (XP SP1) was niet up-to-date

» *preventie*: Microsoft

Vervolgens was ik er nog niet volledig van verlost! Ik kreeg de melding RUNDLL \"Error loading D:\\WINDOWS\\image.dll The specified module could not be found. OK\".

Op hostclub.net vond ik de (engelstalige) oplossing. Hier volgt een beschrijving hoe ik succevol het probleem aan pakte:

Vanuit Windows, klik achtereenvolgens op \'Start\' en \'Run\', type \'regedit\' in en klik op \'OK\'. Vanuit het Registry Editor menu, klik op Edit, dan Find. Type \'image.dll\' in en klik op \'Find Next\'. Er kunnen een paar verschillende plaatsen zijn waar de image.dll bestaat. Degene die we zoeken zit onder de sleutel met de naam \'Run\'. U weet dat u de juiste boosdoener te pakken heeft als u de image.dll Ã © Ã ©n keer aanklikt. Onderaan de Registry Editor verschijnt dan Ã © Ã ©n (of meer) van deze regels:

MyComputer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\ Microsoft\\Windows\\CurrentVersion\\Run
MyComputer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\ Microsoft\\Windows\\CurrentVersion\\ policies\\explorer\\Run

Als u zeker bent dat u de juiste heeft dan ziet u aan de rechterkant van de Registry Editor een lijst. Dit zijn de programma\'s die worden geactiveerd telkens wanneer u uw computer opstart. Zoek de regel met daarin de tekst \'RunDll32.Exe image.dll\', \'RunDll32.EXE image.dll /install\', \"rundll32 C:\\WINDOWS\\image.dll,Install\" of iets wat daar zeer sterk op lijkt.

Klik op deze regel, zorg ervoor dat alleen deze ene regel gemarkeerd is en druk op de \'Delete\' knop om hem te vewijderen. Bevestig eventueel het verwijderen en verlaat daarna de Registry Editor. Start uw computer opnieuw op om uit te testen of de melding nu inderdaad achterwege blijft.

Ziezo, CoolWebSearch definitief gekilled op mijn pc. Case closed.