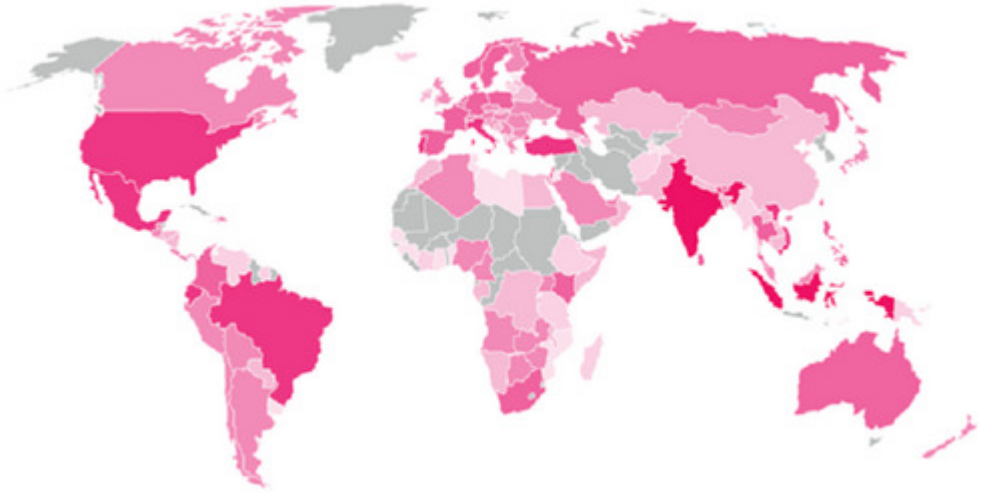
hln.be

Fireball verandert browsers in zombies op meer dan 250 miljoen computers - HLN.be

Steven Alen

5-7 minuten



Zo ontdek je of je besmet bent en hoe je de malware verwijdert

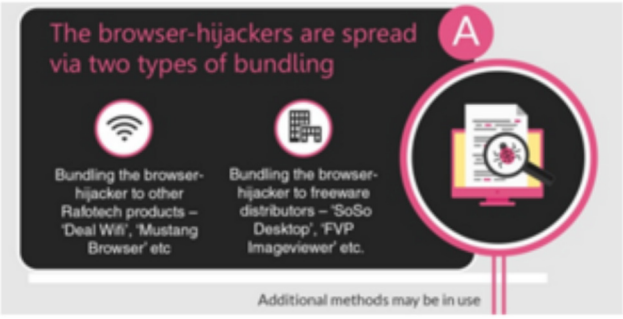
© Check Point.
internet Meer dan 20 procent van bedrijfsnetwerken en meer dan 250 miljoen computers wereldwijd, dat is volgens Check Point Software Technologies het bereik van een nieuwe Chinese malwarecampagne. De IT-beveiliger spreekt van "mogelijk de grootste besmettingsoperatie ooit".

Lees ook

- 22-jarige die WannaCry-aanval stillegde, betreurt zijn 'five minutes of fame'
- Nieuw virus: hackers gebruiken uw computer om virtueel geld te verkrijgen
- "Cyberaanval WannaCry gelinkt aan Noord-Korea"
- "300.000 computers in 150 landen besmet met WannaCry"

Computers worden geïnfecteerd via gratis software die de gebruiker downloadt. De kwaadaardige software komt dan mee in een bundel, vaak zonder toestemming van het slachtoffer.

De malware kreeg de naam Fireball. Volgens de onderzoekteams neemt de software de controle over browsers over en verandert hij die in zombies.
De malware kan identiteitsgegevens stelen, andere kwaadaardige software downloaden en eender welke code draaien op het besmette toestel.

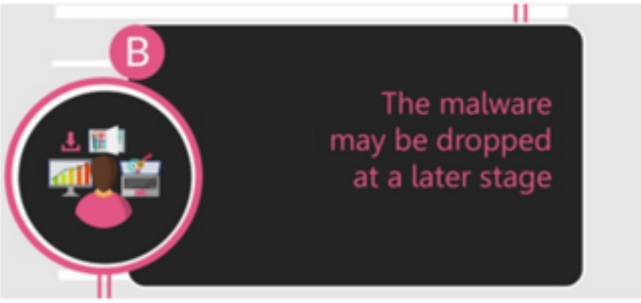


Check Point.

Marketingbedrijf

Fireball kan ook het webverkeer van geïnfecteerde computers kapen en manipuleren om advertentie-inkomsten te genereren, onder meer met valse zoekmachines. Het installeert plug-ins en aanvullende configuraties om de advertentie-inkomsten te boosten.

Volgens Check Point is de dader een Chinees digitaal marketingagentschap met de naam Rafotech. "Hoewel het de verantwoordelijkheid niet toegeeft voor de valse zoekmachines en software om browsers te kapen, noemt het zich ironisch genoeg wel een succesvol marketingbedrijf", meldt Check Point. "Met een bereik van 300 miljoen gebruikers wereldwijd - toevallig gelijkaardig aan ons aantal geschatte infecties."



©

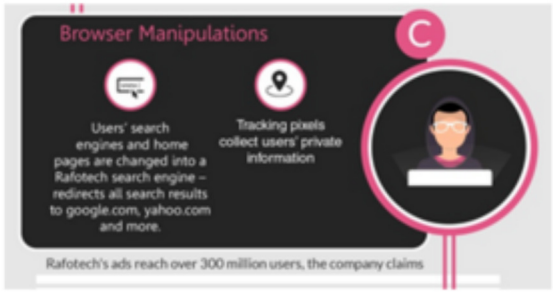
Check Point.

Veel besmettingen

Van de 250 miljoen besmettingen zitten er volgens Check Point 25,3 miljoen in India (10,1 procent), 24,1 miljoen in Brazilië (9,6 procent), 16,1 miljoen in Mexico (6,4 procent) en 13,1 miljoen in Indonesië (5,2 procent). In de Verenigde Staten zijn volgens

Trend Micro 5,5 miljoen toestellen (2,2 procent) besmet.

Op het vlak van bedrijfsnetwerken is de situatie nog erger, met een besmettingsgraad van 20 procent wereldwijd. De 10,7 procent in de Verenigde Staten en 4,7 procent in China vallen op, terwijl de cijfers in Indonesië (60 procent), India (43 procent) en Brazilië (38 procent) nog onthutsender zijn. Bovendien zouden veertien van de valse zoekmachines bij de 10.000 populairste websites zitten, sommige zelfs in de top 1.000.



©

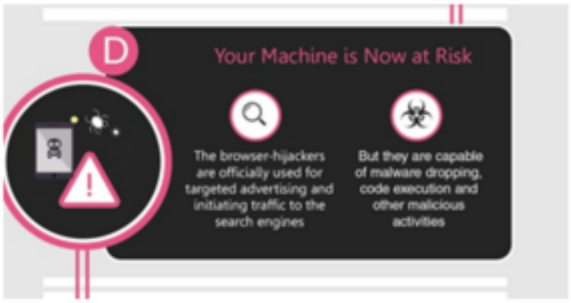
Check Point.

Gevolgen

Het is nog niet duidelijk wat de gevolgen zijn van de besmetting. "Maar het is zeker dat het gaat om een groot gevaar voor het globale cyberecosysteem", luidt het. "Hoewel het niet gaat om een typische malwareaanvalcampagne, geloven we dat Fireball het potentieel heeft om onomkeerbare schade te berokkenen aan slachtoffers en internetgebruikers wereldwijd. " Bovendien vond Check Point nog andere software die browsers kaapt. Een van die bedrijven is ELEX Technology, een internetbedrijf dat net

als Rafotch uit Peking komt en er mogelijk mee verwant is.

Momenteel lijkt Fireball vooral gebruikt te worden voor advertenties en het omleiden van gebruikers naar valse zoekmachines. Maar het kan dus veel meer, met verregaande gevolgen. Rafotech zou gevoelige gegevens van alle besmette computers kunnen oogsten en verkopen, zoals bankkaartgegevens, medische data, patenten en bedrijfsplannen. "Hoe erg is het? Stel je een pesticide voor dat gewapend is met een atoombom", luidt het. "Jazeker, het kan de taak aan. Maar het kan ook veel meer."



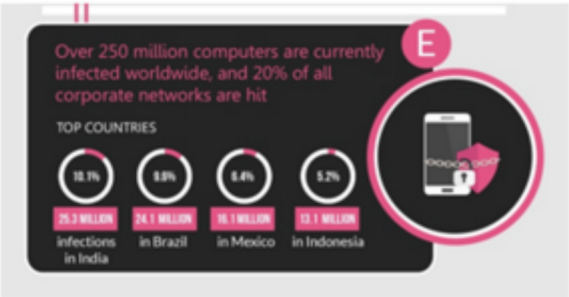
©

Check Point.

Ben je besmet? Zo check je het

Om te controleren of je al dan niet besmet bent, kan je een goede malwarescanner gebruiken. Of je opent je browser en controleert of je de homepage ziet die je zelf hebt gezet. Is je zoekmachine dezelfde als degene die je altijd al hebt gebruikt, en kun je die aanpassen? Heb je al je browserextensies zelf geïnstalleerd? Als het antwoord op een van die vragen negatief

is, dan het je het mogelijk zitten.



©

Check Point.

Hoe verwijder je Fireball?

Naast je computer scannnen met een goed beveiligingsprogramma kan je ook malware verwijderen in het 'Windows Control Panel', bij 'Programs and Features'. Enkele programma's die Rafotech gebruikt zijn 'Deal WiFi', 'Mustang Browser', 'Soso Desktop' en 'FVP Imageviewer'. Macgebruikers kunnen met Finder naar de map 'Applications', waar ze de verdachte bestanden naar de vuilnisbak kunnen slepen.

In de browser kan je verdachte extensies en plug-ins verwijderen, bijvoorbeeld via 'More Tools & Extensions' in Chrome en 'Add-ons' bij Firefox en 'Manage add-ons' bij Internet Explorer. In Safari vind je de 'Extensions'-tab bij 'Preferences'. Je verwijdert best ook alle browserdata en reset de instellingen ervan.

HLN.be-nieuws in je facebook nieuwsfeed?

- reacties (12)

- Bewaar artikel
- Mail
- Print

Rapporteer **een fout in het artikel aan onze redactie**