Malware verstopt zich achter typefouten in topleveldomein

16 maart 2016 16:37

Onderzoekers van het bedrijf Endgame hebben ontdekt dat kwaadwillenden websites opzetten, waarbij er een letter ontbreekt in het topleveldomein. Daarmee hopen ze mensen te lokken die per ongeluk een typefout in een url typen.

Een van de voorbeelden die wordt genoemd is netflix.om, waarbij er dus een c ontbreekt in het TLD. Er zijn meer dan 300 van dergelijke sites geïdentificeerd, waaronder ook youtube.om en twitter.om.

Endgame ontdekte dat het vrij simpel is om zo'n .om-domein op te zetten. Dat komt mede doordat deze domeinen eigenlijk bedoeld zijn voor sites uit Oman, een land in West-Azië.

Overigens waarschuwen browsers in sommige gevallen al dat er iets mis lijkt, als je zo'n adres intypt. Chrome geeft bijvoorbeeld de melding dat 'een misleidende site is gedetecteerd'. 'Typosquatting' is dan ook niet nieuw, maar nog wel *alive and kicking.*

Adware

Kom je op zo'n .om-site terecht, dan laten de sites je een Flash Installer downloaden die in werkelijkheid je computer infecteert met adware. Het virus in kwestie is door de onderzoekers tot 'Genieo' gedoopt.

Bron: Business Insider
URL: http://uk.businessinsider.com/popular-website-typos-like-netflixom-can-infect-your-computer-with-malware-2016-3?r=US&IR=T