Nieuws

Onderzoekers worden via verlopen domeinnaam beheerder .Mobi-domein

woensdag 11 september 2024, 14:39 door **Redactie**, 2 **reacties**

Beveiligingsonderzoekers zijn erin geslaagd om via een verlopen domeinnaam beheerder van het .Mobi generic top-level domain (gTLD) te worden en hadden hier op allerlei manieren misbruik van kunnen maken. Het .Mobi-domein werd in 2005 geïntroduceerd. De Whois-zoekmachine van de gTLD, waarmee informatie over domeinnaamhouders is op te vragen, migreerde een aantal jaren geleden van whois.dotmobiregistry.net naar whois.nic.mobi.

De domeinnaam dotmobiregistry.net verliep afgelopen december en werd door de onderzoekers geregistreerd. Die besloten twee weken geleden een Whois-server aan de whois.dotmobiregistry.net hostname te koppelen. Allerlei partijen bleken nog gebruik te maken van whois.dotmobiregistry.net, waaronder certificaatautoriteiten die verantwoordelijk zijn voor het uitgeven van tls-certificaten voor domeinen zoals 'google.mobi' en 'microsoft.mobi'.

De certificaatautoriteiten gebruikten de Whois-server van de onderzoekers om de domeineigenaren te bepalen en te kijken waar de verificatiedetails naartoe gestuurd moesten worden. Ook zouden via een malafide .Mobi Whois-server allerlei andere aanvallen mogelijk zijn. Na overleg met verschillende partijen besloten de onderzoekers van securitybedrijf **watchTowr Labs** om het dotmobiregistry.net domein en de whois.dotmobiregisry.net hostname naar systemen van The ShadowServer Foundation te laten wijzen, die verzoeken vervolgens naar de legitieme Whois voor het .Mobi-domein doorzetten.

Ivanti Endpoint Manager via kritieke kwetsbaarheid op afstand over te nemen
Douane trekt aanbesteding voor aanschaf mobiele containerscanners in

Reacties (2)

11-09-2024, 19:29 door Anoniem — Reageer met quote

Doet me denken aan **https://thehackerblog.com/the-journey-to-hijacking-a-countrys-tld-the-hidden-risks-of-domain-extensions/** en **https://tweakers.net/nieuws/126993/onderzoeker-kreeg-controle-over-vier-van-zeven-nameservers-van-io-domein.html**.

Voordat je als bedrijf een domein onder een TLD gaat gebruiken of op je website een script laad vanuit wat bijzonderdere TLD's moet je blijkbaar toch maar eens goed gaan kijken of je dat allemaal wel goed genoeg vertrouwd.

12-09-2024, 12:31 door Anoniem — Reageer met quote

Ze worden geen beheerder van het domein, ze hadden alleen controle over een whois server (die informatie over domeinen geeft) maar ze konden niet een domein overnemen op deze wijze. Wel konden de contact informatie veranderen, om zo certificaten te ontvangen of zo of ander misbruik maar geen beheer over het domein zelf, men kon niet de dns of de echte whois aanpassen ...

Reageren

Ondersteunde bbcodes

Je bent niet ingelogd en reageert "**Anoniem**". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je hier direct een account aanmaken. Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.

Nieuwe code

Herhaal code:

Preview Reageren

Altijd meteen op de hoogte van het laatste security nieuws? Volg ons ook op X!

Lees meer