

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 [watchTower 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](#)

Zoeken



Vacature



Rijksoverheid

Information Security Officer (ISO)

Dienst Justitiële Inrichtingen

Ben jij een tech-liefhebber met een passie voor informatiebeveiliging? Wil je jouw expertise inzetten om de veiligheid te waarborgen binnen een dynamische omgeving? Dan is de rol van Informatiebeveiligingsfunctionaris bij Justitieel Complex Zaanstad wellicht jouw volgende avontuur! In deze rol ben jij de sleutel tot het creëren en handhaven van een veilige werkomgeving, waarbij onze organisatie optimaal blijft draaien.

[Lees meer](#) 

Privacyvriendelijke leeftijdsverificatie:

- ☐ Kansloos
- ☐ Het proberen waard
- ☐ ' OR '1'='1

Aantal stemmen: **946**

[17 reacties](#)

Vacature



Gemeente Utrecht

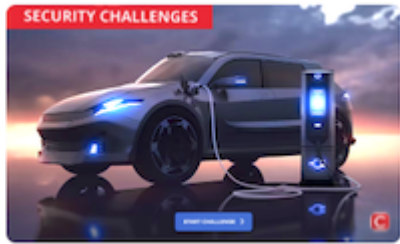
Chief Information Security Officer

Utrecht heeft jou nodig! Als Chief Information Security Officer speel jij een cruciale rol in de bescherming van de digitale informatie van de gemeente Utrecht. Als geen ander weet jij welke dreigingen er zijn en kun je deze vertalen naar risico's die de gemeente en haar inwoners lopen. Solliciteer nu!

[Lees meer](#) 



Vacature



Cybersecurity Trainer / Streamer

Toe aan een nieuwe nieuwe job waarmee je het verschil maakt? In de Certified Secure trainingen laat je deelnemers zien hoe actuele kwetsbaarheden structureel verholpen worden. Ook werk je actief mee aan de ontwikkeling van onze gamified security challenges. Bij het maken van challenges kom je telkens nieuwe technieken tegen, van Flutter tot GraphQL, van Elastic Search tot Kubernetes.

[Lees meer](#) 

Security.NL - X

10-01-2024 door [Redactie](#)

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

[Lees meer](#) 