Privacypolicy

Proactive recognition of domain abuse

Datum
16 juni 2020

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/2

Contact
T 026 352 55 00
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

Naam onderzoek/applicatie	Proactive recognition of domain abuse
Ingangsdatum policy	19 maart 2020
Doel van de applicatie of het onderzoek	Het onderzoek heeft twee doelen: 1. Het verhogen van de detectie van foutieve registratiegegevens voor het .nl-domein. 2. Het verhogen van de veiligheid en weerbaarheid van het .nl-domein door aan de hand van registratiegegevens automatische verdachte registraties te herkennen. Kort samengevat zal de data die gebruikt gaat worden voornamelijk komen uit de DRS-database. De data wordt gekopieerd naar een server binnen het LABS-netwerk zodat ermee gewerkt kan worden. Zodra de train- en testfases van de systemen zijn afgerond, zal de data weer van de server worden verwijderd. Verdere databronnen die nog gebruikt gaan worden zijn takedown notices (deze bevatten de domeinnaam, naam van de houder en de reden van takedown) en eventueel blacklists van derde partijen zoals VirusTotal. Deze blacklists bevatten tijden en URL's van websites die malicious activity hebben vertoond. Voor het creëren van een systeem dat automatisch foute registratiegegevens opspoort, wordt de DRS-database gebruikt. Voor het creëren van een systeem dat automatisch verdachte registraties detecteert, wordt de DRS-database in combinatie met andere blacklists gebruikt. Voor beide systemen wordt de data alleen gebruikt om te testen welke eigenschappen van nieuw-geregistreerde domeinnamen kunnen aantonen dat een registratie fout of zelfs malafide is.

Persoonsgegevens	Registratiegegevens van alle geregistreerde domeinen in het .nl-domein. Dat zijn naam, e-mailadres, telefoonnummer, postcode, straat en huisnummer.
Grondslag	Gerechtvaardigd belang.
Filters	Alle data van de DRS-database en takedown notices (deze bevatten de domeinnaam, naam van de houder en de reden van takedown) worden gebruikt om de systemen te trainen en testen. Zodra wordt vastgesteld dat bepaalde data in de dataset niet relevant meer is voor het onderzoek wordt deze ook niet meer gebruikt en wordt deze data verwijderd. Data is niet meer relevant zodra is vastgesteld dat het de prestatie van de systemen niet beter maakt.
Retentie	Eventuele nieuwe databronnen (zoals blacklists van 3e partijen) worden alleen gebruikt om de systemen te trainen en testen. Deze databronnen bevatten geen persoonlijke informatie. Zodra deze fase voorbij is, wordt deze data ook verwijderd. De verwachting is dat de train- en testfase ongeveer 4 maanden in beslag neemt. De gecreëerde systemen bevatten zelf geen persoonlijke informatie. Echter verwerken deze systemen wel nieuw binnenkomende registratiedata.
Toegang	Iedereen van SIDN Labs. De data (DRS-database, takedown notices, en eventuele blacklists) worden op een server opgeslagen die is beschermd door middel van persoonsgebonden 2F-authenticatie (TOTP voor SSH en client-certificaten voor web, naast username wachtwoord combinatie).
Publicatie/delen	Over het onderzoek wordt een master thesis geschreven. Hierin wordt de prestatie van de systemen gerapporteerd en zal geen persoonlijke informatie bevatten.
Type	R&D Onderzoek en prototype
Andere beveiligingsmaatregelen	Geen.